ZyWALL (ZyNOS) CLI Reference Guide

Internet Security Appliance

CLI Reference Guide

Version 4.04
4/2008
Edition 1

DEFAULT LOGIN	
In-band IP Address	**http://192.168.1.1**
User Name	**admin**
Password	**1234**

www.zyxel.com

About This CLI Reference Guide

Intended Audience

This manual is intended for people who want to configure the ZyWALL via Command Line Interface (CLI). You should have at least a basic knowledge of TCP/IP networking concepts and topology.

> This guide is intended as a command reference for a series of products. Therefore many commands in this guide may not be available in your product. See your User's Guide for a list of supported features and details about feature implementation.

Please refer to www.zyxel.com or your product's CD for product specific User Guides and product certifications.

How To Use This Guide

- Read Chapter 1 on page 13 for an overview of various ways you can get to the command interface on your ZyWALL.
- Read Chapter 2 on page 17 for an introduction to some of the more commonly used commands.

> It is highly recommended that you read at least these two chapters.

- The other chapters in this guide are arranged according to the CLI structure. Each chapter describes commands related to a feature.

> See your ZyWALL's User Guide for feature background information.

- To find specific information in this guide, use the **Contents Overview**, the **Index of Commands**, or search the PDF file. E-mail techwriters@zyxel.com.tw if you cannot find the information you require.

CLI Reference Guide Feedback

Help us help you. Send all guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

Warnings and notes are indicated as follows in this guide.

Warnings tell you about things that could harm you or your device. See your User's Guide for product specific warnings.

Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

This manual follows these general conventions:

- ZyWALLs may also be referred to as the "device", the "ZyXEL device", the "system" or the "product" in this guide.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.

Command descriptions follow these conventions:

- Commands are in `courier new font`.
- Required input values are in angle brackets <>; for example, `ping <ip-address>` means that you must specify an IP address for this command.
- Optional fields are in square brackets []; for instance `show logins [name]`, the name field is optional.

  The following is an example of a required field within an optional field: `snmp-server [contact <system contact>]`, the `contact` field is optional. However, if you use `contact`, then you must provide the `system contact` information.
- The `|` (bar) symbol means "or".
- *`italic`* terms represent user-defined input values; for example, in `sys datetime date [year month date]`, *`year month date`* can be replaced by the actual year month and date that you want to set, for example, 2007 08 15.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "Enter" or "Return" key on your keyboard.
- `<cr>` means press the [ENTER] key.
- An arrow (`-->`) indicates that this line is a continuation of the previous line.

Command summary tables are organized as follows:

Table 1 Table Title

COMMAND	DESCRIPTION	M
`ip alg disable <ALG_FTP|ALG_H323|ALG_SIP>`	Turns off the specified ALG (Application Layer Gateway).	R+B
`ip alg disp`	Shows whether the ALG is enabled or disabled.	R+B
`ip alg enable <ALG_FTP|ALG_H323|ALG_SIP>`	Turns on the specified ALG.	R+B
`ip alg ftpPortNum [`*`port`*`]`	Sets the FTP ALG to support a different port number (instead of the default).	R+B
`ip alg siptimeout <`*`timeout`*`>`	Sets the SIP timeout in seconds. 0 means no timeout.	R+B
`ip alias <`*`interface`*`>`	Sets an alias for the specified interface.	R

The **Table** title identifies commands or the specific feature that the commands configure.

The **COMMAND** column shows the syntax of the command.

The **DESCRIPTION** column explains what the command does. It may also identify legal input values.

The **M** column identifies the mode in which you run the command.

- **R**: The command is available in router mode.
- **B**: The command is available in bridge mode.
- **R + B**: The command is available in both router and bridge modes

A long list of pre-defined values may be replaced by a command input value ‘variable’ so as to avoid a very long command in the description table. Refer to the command input values table if you are unsure of what to enter.

Table 2 Common Command Input Values

LABEL	DESCRIPTION
`description`	Used when a command has a description field in order to add more detail.
`ip-address`	An IP address in dotted decimal notation. For example, 192.168.1.3.
`mask`	The subnet mask in dotted decimal notation, for example, 255.255.255.0.
`mask-bits`	The number of bits in an address’s subnet mask. For example type /24 for a subnet mask of 255.255.255.0.
`port`	A protocol’s port number.

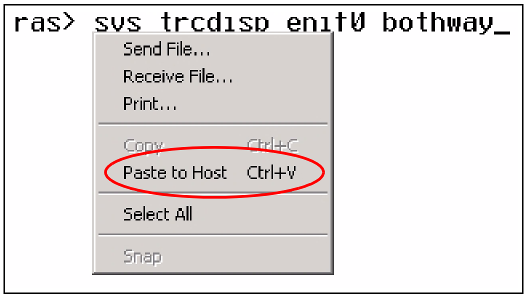
Table 2 Common Command Input Values (continued)

LABEL	DESCRIPTION
interface	An interface on the ZyWALL. Use the following for a ZyWALL with a single WAN Ethernet interface. enif0: LAN enif1: Ethernet WAN enif2: DMZ enif4: Ethernet WLAN wanif0: PPPoE or PPTP or 3G depending on which is connected first wanif1: PPPoE or PPTP or 3G depending on which is connected second Use the following for a ZyWALL with two WAN Ethernet interfaces. enif0: LAN enif1: Ethernet WAN 1 enif2: DMZ enif3: Ethernet WAN 2 enif5: Ethernet WLAN wanif0: PPPoE or PPTP or 3G depending on which is connected first wanif1: PPPoE or PPTP or 3G depending on which is connected second For some commands you can also add a colon and a 0 or 1 to specify an IP alias. This is only for the LAN, DMZ, and WLAN interfaces. For example, enif0:0 specifies LAN IP alias 1 and enif0:1 specifies LAN IP alias 2.
hostname	Hostname can be an IP address or domain name.
name	Used for the name of a rule, policy, set, group and so on.
number	Used for a number, for example 10, that you have to input.

Commands are case sensitive! Enter commands exactly as seen in the command interface. Remember to also include underscores if required.

Copy and Paste Commands

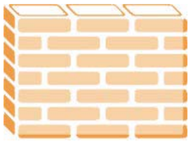
You can copy and paste commands directly from this document into your terminal emulation console window (such as HyperTerminal). Use right-click (not ctrl-v) to paste your command into the console window as shown next.



```
ras> sys trcdisp enif0 bothway_
```

Icons Used in Figures

Figures in this guide may use the following generic icons. The ZyWALL icon is not an exact representation of your device.

ZyWALL 	Computer 	Notebook computer
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router

Contents Overview

PART I
Introduction

How to Access and Use the CLI

This chapter introduces the command line interface (CLI).

1.1 Accessing the CLI

Use any of the following methods to access the CLI.

1.1.1 Console Port

You may use this method if your ZyWALL has a console port.

1. Connect your computer to the console port on the ZyWALL using the appropriate cable.
2. Use terminal emulation software with the following settings:

Table 3 Default Settings for the Console Port

SETTING	DEFAULT VALUE
Terminal Emulation	VT100
Baud Rate	9600 bps
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

3. Press [ENTER] to open the login screen.

1.1.2 Telnet

4. Open a Telnet session to the ZyWALL's IP address. If this is your first login, use the default values.

Table 4 Default Management IP Address

SETTING	DEFAULT VALUE
IP Address	192.168.1.1
Subnet Mask	255.255.255.0

Make sure your computer IP address is in the same subnet, unless you are accessing the ZyWALL through one or more routers. In the latter case, make sure remote management of the ZyWALL is allowed via Telnet.

1.1.3 SSH

You may use this method if your ZyWALL supports SSH connections.

1. Connect your computer to one of the Ethernet ports.
2. Use a SSH client program to access the ZyWALL. If this is your first login, use the default values in Table 4 on page 13 and Table 5 on page 14. Make sure your computer IP address is in the same subnet, unless you are accessing the ZyWALL through one or more routers.

1.2 Logging in

Use the administrator username and password. If this is your first login, use the default values. in some ZyWALLs you may not need to enter the user name.

Table 5 Default User Name and Password

SETTING	DEFAULT VALUE
User Name	admin
Password	1234

The ZyWALL automatically logs you out of the management interface after five minutes of inactivity. If this happens to you, simply log back in again. Use the `sys stdio` command to extend the idle timeout. For example, the ZyWALL automatically logs you out of the management interface after 60 minutes of inactivity after you use the `sys stdio 60` command.

1.3 Using Shortcuts and Getting Help

This table identifies some shortcuts in the CLI, as well as how to get help.

Table 6 CLI Shortcuts and Help

COMMAND / KEY(S)	DESCRIPTION
↑↓ `(up/down arrow keys)`	Scrolls through the list of recently-used commands. You can edit any command or press `[ENTER]` to run it again.
`[CTRL]+U`	Clears the current command.
?	Displays the keywords and/or input values that are allowed in place of the ?.
`help`	Displays the (full) commands that are allowed in place of `help`.

Use the `help` command to view the available commands on the ZyWALL. Follow these steps to create a list of supported commands:

1. Log into the CLI.

2 Type `help` and press [ENTER]. A list comes up which shows all the commands available for this device.

```
ras> help
Valid commands are:
sys             exit            ether           aux
config          wwan            wlan            ip
ipsec           bridge          bm              certificates
8021x           radius          radserv         wcfg
ras>
```

Abbreviations

Commands can be abbreviated to the smallest unique string that differentiates the command. For example `sys version` could be abbreviated to `s v`.

```
ras> sys version

 ZyNOS version: V4.03(XD.0)Preb2_0802_1 | 08/03/2007
 romRasSize: 3596736
 system up time:    42:41:02 (ea784b ticks)
 bootbase version: V1.08 | 01/28/2005
 CPU chip revision: 1
 CPU chip clock: 266MHz
 CPU core revision: 0
ras> s v

 ZyNOS version: V4.03(XD.0)Preb2_0802_1 | 08/03/2007
 romRasSize: 3596736
 system up time:    42:41:05 (ea796a ticks)
 bootbase version: V1.08 | 01/28/2005
 CPU chip revision: 1
 CPU chip clock: 266MHz
 CPU core revision: 0
ras>
```

1.4 Saving Your Configuration

In the ZyWALL some commands are saved as you run them and others require you to run a save command. For example, type `ip stroute save` to save the static route rule in non-volatile memory. See the related section of this guide to see if a save command is required.

Unsaved configuration changes to commands that require you to run a save command are lost once you restart the ZyWALL

1.5 Logging Out

Enter `exit` to log out of the CLI.

Table 7 Exit Command

COMMAND	DESCRIPTION	M
`exit`	Logs you out of the CLI.	R+B

2

Common Commands

This chapter introduces some of the more commonly-used commands in the ZyWALL. For more detailed usage, see the corresponding feature chapter in this guide.

In the following examples, `ras` is the prompt as that is the default. If you configure a system name, then that prompt will display as the system name you configured. For example, change the system name to `zyxel` using the `sys hostname zyxel` command; the command prompt will then display as `zyxel>`.

2.1 Change the Idle Timeout

By default, the ZyWALL automatically logs you out of the management interface after five minutes of inactivity. Use the `sys stdio` command to extend the idle timeout. The following example extends the idle timeout to 120 minutes.

```
ras> sys stdio 120
Stdio Timeout = 120 minutes
ras>
```

2.2 Interface Information

ZyWALL interfaces are defined as shown in Table 2 on page 6.

The first command in this example shows information about the LAN port, for example, it has an IP address of 192.168.1.1. The second command is used to change this IP address to 192.168.100.100.

```
ras> ip ifconfig enif0
enif0: mtu 1500 mss 1460
    inet 192.168.1.1, netmask 0xffffff00, broadcast 192.168.1.255
    RIP RX:Ver 1 & 2, TX:Ver 1,
    [InOctets            0] [InUnicast        0] [InMulticast           0]
    [InDiscards          0] [InErrors         0] [InUnknownProtos       0]
    [OutOctets         156] [OutUnicast       0] [OutMulticast          3]
    [OutDiscards          0] [OutErrors         0]
ras> ip ifconfig enif0 192.168.100.100/24
enif0: mtu 1500 mss 1460
    inet 192.168.100.100, netmask 0xffffff00, broadcast 192.168.100.255
    RIP RX:Ver 1 & 2, TX:Ver 1,
    [InOctets            0] [InUnicast        0] [InMulticast           0]
    [InDiscards          0] [InErrors         0] [InUnknownProtos       0]
    [OutOctets         728] [OutUnicast       0] [OutMulticast         14]
    [OutDiscards          0] [OutErrors         0]
ras>
```

Afterwards, you have to use this new IP address to access the ZyWALL via the LAN port.

To view information on all interfaces, enter `ip ifconfig`.

To view DHCP information on the LAN port, enter `ip dhcp enif0 status`.

```
ras> ip dhcp enif0 status
DHCP on iface enif0 is server
     Start assigned IP address: 192.168.1.33/24
     Number of IP addresses reserved: 128
     Hostname prefix: dhcppc
     DNS server: 0.0.0.0 0.0.0.0 0.0.0.0
     WINS server: 0.0.0.0 0.0.0.0
     Domain Name :
     Default gateway: 192.168.1.1
     Lease time: 259200 seconds
     Renewal time: 129600 seconds
     Rebind time: 226800 seconds
     Probing count: 4
     Probing type: ICMP
slot    state      timer   type hardware address      hostname
   0  UNCERTAIN          0    0  00
   1  UNCERTAIN          0    0  00
```

Use these commands to release and renew DHCP-assigned information on the specified interface.

```
ras> ip dhcp enif1 client release
ras> ip dhcp enif1 status
DHCP on iface enif1 is client
     Hostname : zyxel.zyxel.com
     Domain Name : zyxel.com
     Server IP address: 0.0.0.0
     Client IP address: 0.0.0.0/27
     DNS server : 0.0.0.0, 0.0.0.0
     Default gateway: 0.0.0.0
     Lease time  : 0 seconds
     Renewal time: 0 seconds
     Rebind time : 0 seconds
     Client State =          8, retry =          0
     periodtimer  =        286, timer =          0
     flags        =          2
Status:
     Packet InCount: 3, OutCount: 3, DiscardCount: 0
ras> ip dhcp enif1 client renew
ras> ip dhcp enif1 status
DHCP on iface enif1 is client
     Hostname : zyxel.zyxel.com
     Domain Name : zyxel.com
     Server IP address: 172.16.5.2
     Client IP address: 172.16.37.48/24
     DNS server : 172.16.5.2, 172.16.5.1, 0.0.0.0
     Default gateway: 172.16.37.254
     Lease time  : 604800 seconds
     Renewal time: 302400 seconds
     Rebind time : 529200 seconds
     Client State =          3, retry =          0
     periodtimer  =        272, timer =     302397
     flags        =          2
Status:
     Packet InCount: 3, OutCount: 2, DiscardCount: 0
```

To view the ARP table for the LAN port, enter `ip arp status enif0`.

```
ras> ip arp status enif0
received 1458 badtype 0 bogus addr 0 reqst in 312 replies 9 reqst out 16
cache hit 11278 (88%), cache miss 1521 (11%)
IP-addr         Type           Time  Addr              stat iface
172.16.1.44    10 Mb Ethernet 290   00:13:49:6b:10:55 41   enif0
172.16.1.123   10 Mb Ethernet 290   00:0a:e4:06:11:91 41   enif0
172.16.1.3     10 Mb Ethernet 290   00:02:e3:57:ea:4f 41   enif0
172.16.1.122   10 Mb Ethernet 280   00:c0:a8:fa:e9:27 41   enif0
172.16.1.105   10 Mb Ethernet 280   00:0f:fe:0a:2d:3b 41   enif0
172.16.1.30    10 Mb Ethernet 270   00:60:b3:45:2b:c5 41   enif0
172.16.1.53    10 Mb Ethernet 210   00:16:d3:b8:3d:1a 41   enif0
172.16.1.32    10 Mb Ethernet 160   00:16:36:10:26:2d 41   enif0
172.16.1.2     10 Mb Ethernet 130   00:16:d3:37:c7:33 41   enif0
172.16.1.42    10 Mb Ethernet 150   00:00:e8:71:e3:f9 41   enif0
172.16.1.14    10 Mb Ethernet 250   00:13:49:fb:99:16 41   enif0
172.16.1.7     10 Mb Ethernet 190   00:0d:60:cb:fd:08 41   enif0
172.16.1.52    10 Mb Ethernet 130   00:0f:fe:32:b4:12 41   enif0
num of arp entries= 13
```

Each ZyWALL can support a specific number of NAT sessions in total. You can limit the number of NAT sessions allowed per host by using the `ip nat session` command. In the following example, each host may have up to 4000 NAT sessions open at one time. The total number of NAT sessions must not exceed the number for your ZyWALL.

```
ras> ip nat session 4000
     ip nat session
NAT session number per host: 4000
ras>
```

To see the IP routing table, enter the following command.

```
ras> ip route status
Dest            FF Len Device     Gateway         Metric stat Timer  Use
192.168.1.0     00 24  enet0      192.168.1.1       1    041b 0      0
192.168.100.0   00 24  enet0      192.168.100.100   1    041b 0      0
default         00 0   Idle       WAN 2             102  002b 0      0
ras>
```

2.3 Basic System Information

Use the following `sys version` and `sys atsh` commands to view information about your ZyWALL.

```
ras> sys version
 ZyNOS version: V4.03(XD.0)Preb2_0802_1 | 08/03/2007
 romRasSize: 3596736
 system up time:    23:51:53 (831816 ticks)
 bootbase version: V1.08 | 01/28/2005
 CPU chip revision: 1
 CPU chip clock: 266MHz
 CPU core revision: 0
```

```
ras> sys atsh
 ZyNOS version : V4.03(XD.0)Preb2_0802_1 | 08/03/2007
 Ram Size : 32768 Kbytes
 Flash Size : Intel 64M * 1
 romRasSize : 3596736
 bootbase version : V1.08 | 01/28/2005
 Vendor Name : ZyXEL Communications Corp.
 Product Model : ZyWALL 5
 MAC Address : 001349000001
 Default Country Code : FF
 Boot Module Debug Flag : 0
 RomFile Version : 38
 RomFile Checksum : b4fc
```

Use the following command to view CPU utilization.

```
ras> sys cpu display
CPU usage status:
  baseline 1472882 ticks
 sec   ticks   load  sec   ticks   load sec   ticks   load  sec  ticks   load
   0 1393404   5.39   1 1472882   0.00    2 1472882   0.00   3 1472882   0.00
   4 1097036  25.51   5 1455444   1.18    6 1460440   0.84   7 1469623   0.22
   8 1472882   0.00   9 1458718   0.96   10   15369  98.96  11  721711  51.00
  12 1462602   0.69  13 1465369   0.51   14 1464771   0.55  15 1469584   0.22
  16 1472882   0.00  17 1472882   0.00   18 1465200   0.52  19 1459341   0.91
  20 1457914   1.01  21 1454838   1.22   22 1472882   0.00  23 1472882   0.00
  24 1458275   0.99  25 1472882   0.00   26 1472882   0.00  27 1472882   0.00
  28 1472882   0.00  29 1472882   0.00   30 1472882   0.00  31 1472882   0.00
  32 1472882   0.00  33 1472882   0.00   34 1472882   0.00  35 1472882   0.00
  36 1472882   0.00  37 1472882   0.00   38 1472882   0.00  39 1460334   0.85
  40 1472882   0.00  41 1472882   0.00   42 1472882   0.00  43 1472882   0.00
  44 1472882   0.00  45 1472882   0.00   46 1472882   0.00  47 1472882   0.00
  48 1472882   0.00  49 1472882   0.00   50 1472882   0.00  51 1472882   0.00
  52 1472882   0.00  53 1472882   0.00   54 1459578   0.90  55 1472882   0.00
  56 1472882   0.00  57 1472882   0.00   58 1472882   0.00  59 1472882   0.00
  60 1472882   0.00  61 1472882   0.00   62 1472882   0.00
Average CPU Load = 3.5%
ras>
```

Use the following command to view the ZyWALL’s time and date.

```
ras> sys datetime time
Current time is 08:26:56
ras> sys datetime date
Current date is Wed 2007/08/08
ras>
```

Use the following command to restart your ZyWALL right away.

```
ras> sys reboot

Bootbase Version: V1.08 | 01/28/2005 14:47:16
RAM:Size = 32 Mbytes
FLASH: Intel 64M

ZyNOS Version: V4.03(XD.0)Preb2_0802_1 | 08/03/2007 16:48:04

Press any key to enter debug mode within 3 seconds.
............................................................
```

Use the following command to reset the ZyWALL to the factory defaults. Make sure you back up your current configuration first (using the web configurator or SMT). The ZyWALL will restart and the console port speed will also reset to 9,600 bps.

```
ras> sys romreset
Do you want to restore default ROM file(y/n)?y
..................................................................OK

System Restart! (Console speed will be changed to 9600 bps)

Bootbase Version: V1.08 | 01/30/2005 14:41:51
RAM:Size = 64 Mbytes
FLASH: Intel 128M

ZyNOS Version: V4.03(WZ.0)Preb2_0803 | 08/03/2007 11:08:13

Press any key to enter debug mode within 3 seconds.
............................................................
```

Use the following command to change the console port speed. A higher console port speed is recommended when uploading firmware via the console port. A console port speed of 115,200 bps is necessary to view CNM debug messages and packet traces on the ZyWALL.

```
ras> sys baud ?
Usage: baud <1..5>(1:38400, 2:19200, 3:9600, 4:57600, 5:115200)
ras> sys baud 5

Saving to ROM.  Please wait...
Change Console Speed to 115200. Then hit any key to continue
ras>
```

After you change the console port speed, you need to change it also on your terminal emulation software (such as HyperTerminal) in order to reconnect to the ZyWALL.

Use the following command to see whether the ZyWALL is acting act as a bridge or router

```
ras> sys mode
Device mode: router
ras>
```

Use the following command to change the ZyWALL mode (bridge or router).

```
Usage: sys mode <router | bridge>
ras> sys mode router
Device mode: router
ras>
```

Use the following command to display all ZyWALL logs. Logs are very useful for troubleshooting. If you are having problems with your ZyWALL, then customer support may request that you send them the logs.

```
ras> sys logs display

#  .time                   notes
    source                 destination
    message
============================================================
  0|2007-08-16 09:39:27   |WAN1
                          |
    WAN interface gets IP:172.16.17.48
  1|2007-08-16 09:38:40   |User:admin
                          |
    Successful SMT login
  2|2007-08-16 09:38:37   |User:admin
                          |
    SMT login failed (password error)
  3|2007-08-16 09:35:10   |
    80.85.129.103:123     |172.16.17.48:1135
    Time set from NTP server: 0.pool.ntp.org, offset: +208949688 sec
  4|2001-01-01 00:00:18   |WAN1
                          |
    WAN interface gets IP:172.16.17.48
  5|2001-01-01 00:00:16   |WAN1
                          |
    WAN1 connection is up.
  6|2001-01-01 00:00:16   |WAN2
                          |
    WAN2 connection is down.

ras>
```

Use the following command to display all ZyWALL error logs

```
ras> sys logs errlog disp
  47 Mon Jan  1 00:00:03 2001 PINI  INFO  Channel 0 ok
  48 Mon Jan  1 00:00:25 2001 PP0e  INFO  LAN promiscuous mode <0>
  51 Mon Jan  1 00:00:25 2001 PINI  INFO  main: init completed
  52 Mon Jan  1 00:00:25 2001 PP22  INFO  No DNS server available
  53 Mon Jan  1 00:11:53 2001 PINI  INFO  Last errorlog repeat 114 Times
  54 Mon Jan  1 00:11:53 2001 PINI  INFO  SMT Session Begin
  55 Mon Jan  1 00:15:25 2001 PP22  INFO  No DNS server available
  56 Mon Jan  1 00:51:15 2001 PINI  INFO  Channel 0 ok
  57 Mon Jan  1 00:51:37 2001 PP0e  INFO  LAN promiscuous mode <0>
  60 Mon Jan  1 00:51:37 2001 PINI  INFO  main: init completed
  61 Mon Jan  1 00:51:37 2001 PP22  INFO  No DNS server available
  62 Mon Jan  1 00:51:41 2001 PINI  INFO  SMT Session Begin
  63 Mon Jan  1 00:52:37 2001 PP1c  INFO  No DNS server available
Clear Error Log (y/n):
```

Use the following commands for system debugging. A console port speed of 115,200 bps is necessary to view packet traces on the ZyWALL.

```
ras> sys trcpacket sw on
ras> sys trcdisp brief
   0 09:21:27.180 ENET1-T[0342] UDP 0.0.0.0:68->255.255.255.255:67
   1 09:21:30.180 ENET1-T[0342] UDP 0.0.0.0:68->255.255.255.255:67
   2 09:21:37.180 ENET1-T[0342] UDP 0.0.0.0:68->255.255.255.255:67
   3 09:21:53.180 ENET1-T[0342] UDP 0.0.0.0:68->255.255.255.255:67
   4 09:21:55.180 ENET1-T[0342] UDP 0.0.0.0:68->255.255.255.255:67
ras> sys trcdisp enif0 bothway

TIME:09:24:53.180  enet1-XMIT len:342 call=0
  0000: ff ff ff ff ff ff 00 13 49 00 00 02 08 00 45 00
  0010: 01 48 04 df 00 00 ff 11 b5 c6 00 00 00 00 ff ff
  0020: ff ff 00 44 00 43 01 34 e6 79 01 01 06 00 00 00
  0030: 1f 4f 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0040: 00 00 00 00 00 00 00 13 49 00 00 02 00 00 00 00
  0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

The extended ping command is used to have the ZyWALL ping IP address 172.16.1.202 five times in the following example.

```
ras> ip pingext 172.16.1.202  -n 5
Resolving 172.16.1.202 ... 172.16.1.202
      sent      rcvd    size     rtt     avg     max     min
         1         1      36     510     510     510     510
         2         2      36     530     520     530     510
         3         3      36     850     630     850     510
         4         4      36    1030     730    1030     510
         5         5      36    1070     798    1070     510

Extended Ping From device to 172.16.1.202:
   Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate Round Trip Times in milli-seconds:
   RTT: Average = 798ms, Maximum =  1070ms, Minimum = 510ms
ras>
```

2.4 UTM and myZyXEL.com

Use these commands to create an account at myZyXEL.com and view what services you have activated.

Ensure your ZyWALL is connected to the Internet before you use the following commands.

You need to create an account at my ZyXEL.com in order to activate content filtering, anti-spam and anti-virus UTM (Unified Threat Management) services. See the myZyXEL.com chapter for information on the country code you should use.

```
ras> sys myZyxelCom register <username> <password> <email> <countryCode>
```

This command displays your ZyWALL's registration information.

```
ras> sys myZyxelCom display

register server address : www.myzyxel.com
register server path : /register/registration?

username : aseawfasf
password : aaaaaa

email : aa@aa.aa.aa

sku : CFRT=1&CFST=319&ZASS=469&ISUS=469&ZAVS=469

country code : 204

register state 1

register MAC : 0000AA220765
CF expired day : 2008-05-26 14:58:19
AS expired day : 2008-10-23 14:58:19
2In1 expired day : 2008-10-23 14:58:19
Last update day : 2007-07-12 14:58:19
```

This command displays ZyWALL service registration details.

```
ras> sys myZyxelCom serviceDisplay
Content Filter Service :
Actived, Licenced, Trial, Expired : 2007-07-08 16:36:15
Anti-Spam Service :
Actived, Licenced, Trial, Expired : 2007-09-06 16:36:18
IDP/Anti-Virus Service :
Actived, Licenced, Trial, Expired : 2007-09-06 16:36:18
ras>
```

Use these commands to enable anti-spam on the ZyWALL for traffic going from WAN1 to LAN.

```
ras> as enable 1
Anti spam: enabled

ras> as dir wan1 lan on
From\To  lan  wan1 dmz  wan2 wlan vpn
=======================================
lan      off  off  off  off  off  off
wan1     on   off  off  off  off  off
dmz      off  off  off  off  off  off
wan2     off  off  off  off  off  off
wlan     off  off  off  off  off  off
vpn      off  off  off  off  off  off
ras>
```

Use the following commands to enable anti-virus on the ZyWALL You first need to use the load command.

```
ras> av load
ras> av config enable on
ras> av save
ras> av disp
 AV Enable : On
 AV Forward Over ZIP Session : Off
 AV Forward Over ZIP Session : Off
------------------------------------
```

Use the following commands to enable content filtering on the ZyWALL, then on the external database (DB) and then display the default policy.

```
ras> ip cf common enable on
ras> ip cf externalDB enable on
ras> ip cf policy displayAll
   index  Name           Active    IP Group
                                   Start Addr End Addr
==========================================================================

    1  Default Policy       Y       0.0.0.0/0.0.0.0
```

The default policy does not actually block anything. Use the following commands to edit the default policy, turn the external database service content filtering (category-based content filtering), see what the categories are, block a category 92 in the following example) and then save the policy.

```
ras> ip cf policy edit 1
ras> ip cf policy config webControl enable on
ras> ip cf policy config webControl display
The Categories:
type 1        :Adult/Mature Content
type 2        :Pornography
type 3        :Sex Education
type 4        :Intimate Apparel/Swimsuit
type 5        :Nudity
type 6        :Alcohol/Tobacco
type 7        :Illegal/Questionable
type 8        :Gambling
type 9        :Violence/Hate/Racism
type10        :Weapons
type11        :Abortion
type12        :Hacking
type13        :Phishing
type14        :Arts/Entertainment
type15        :Business/Economy
type16        :Alternative Spirituality/Occult
type17        :Illegal Drugs
type18        :Education
type19        :Cultural/Charitable Organization
type20        :Financial Services
type21        :Brokerage/Trading
type22        :Online Games
type23        :Government/Legal
type24        :Military
type25        :Political/Activist Groups
type26        :Health
type27        :Computers/Internet
type28        :Search Engines/Portals
type29        :Spyware/Malware Sources
type30        :Spyware Effects/Privacy Concerns
type31        :Job Search/Careers
type32        :News/Media
type33        :Personals/Dating
type34        :Reference
type35        :Open Image/Media Search
type36        :Chat/Instant Messaging
type37        :Email
type38        :Blogs/Newsgroups
type39        :Religion
type40        :Social Networking
type41        :Online Storage
type42        :Remote Access Tools
type43        :Shopping
type44        :Auctions
type45        :Real Estate
type46        :Society/Lifestyle
type47        :Sexuality/Alternative Lifestyles
type48        :Restaurants/Dining/Food
type49        :Sports/Recreation/Hobbies
type50        :Travel
type51        :Vehicles
type52        :Humor/Jokes
type53        :Software Downloads
type54        :Pay to Surf
type55        :Peer-to-Peer
type56        :Streaming Media/MP3s
type57        :Proxy Avoidance
type58        :For Kids
type59        :Web Advertisements
type60        :Web Hosting
type61        :Unrated
ras> ip cf policy config webControl category block 2
The Categories:
type 1        :Adult/Mature Content
type 2 (block):Pornography
-------
ras> ip cf policy save
ras>
```

You may also configure and schedule new policies using commands as well as configure what to block using the external database.

2.5 Firewall

Use the following command to enable the firewall on the ZyWALL.

```
ras> sys firewall active yes
ras>
```

2.6 VPN

Use the following command to show what IPsec VPN tunnels are active on your ZyWALL.

```
ras> ipsec show_runtime sa
Runtime SA status:

No phase 1 IKE SA exist
No phase 2 IPSec SA exist
Active SA pair = 0

ras>
```

Use the following command to manually bring up a previously configured VPN tunnel.

```
ras> ipsec dial 1
Start dialing for tunnel <rule# 1>...
.....................
```

2.7 Dialing PPPoE and PPTP Connections

This example shows dialing up remote node “WAN 1” using PPPoE.

```
ras> poe dial "WAN 1"
Start dialing for node <WAN 1>...
### Hit any key to continue.###
$$$ DIALING dev=6 ch=0..........
$$$ OUTGOING-CALL phone()
$$$ CALL CONNECT speed<100000000> type<6> chan<0>
$$$ LCP opened
$$$ PAP sending user/pswd
$$$ IPCP negotiation started
$$$ IPCP neg' Primary DNS 192.168.30.1
$$$ IPCP neg' Primary DNS 172.16.5.2
$$$ IPCP opened
```

This example shows dialing up remote node “WAN 1” using PPTP.

```
ras> pptp dial "WAN 1"
Start dialing for node <WAN 1>...
### Hit any key to continue.###


ras>
```

PART II
Reference

3

Antispam Commands

Use these commands to configure antispam settings on the ZyWALL.

3.1 Command Summary

The following table describes the values required for many antispam (as) commands. Other values are discussed with the corresponding commands.

Table 8 as Command Input Values

LABEL	DESCRIPTION
interface	Specifies an interface. The options are lan|wan1|dmz|wlan|vpn (not case sensitive)
number, start-number, end-number	Specifies an index number less than or equal to the total number of entries on a black or white list.
timeout	Specifies the timeout period in seconds.

The following section lists the commands for this feature.

.

Table 9 as Commands

COMMAND	DESCRIPTION	M
as asAction [0|1]	When the mail session limit has been exceeded the ZyWALL either forwards further mail to recipients (0) or blocks further mail (1).	R+B
as delete blackRule <*number*|*start-number*>[*end-number*]	Deletes the blacklist filter. The user can delete one filter or a set of filters.	R+B
as delete whiteRule <*number*|*start-number*>[*end-number*]	Deletes the whitelist filter. The user can delete one filter or a set of filters.	R+B
as dir <*interface*><*interface*><on|off>	Enables or disables antispam checking depending on the source and destination of the mail.	R+B
as display antispam	Displays the antispam configuration.	R+B
as display runtimedata <all|black|white> [all|ip|mime|email|subject]	Displays runtime data for the antispam ACL (Access Control List) structure.	R+B
as display serverlist	Displays the list of rating servers. The rating server provides a score for each mail on how likely it is to be spam or not.	R+B
as enable <0|1>	Enables (1) or disables (0) antispam.	R+B

Table 9 as Commands (continued)

COMMAND	DESCRIPTION	M
as failTolerance [*timeout*]	Sets the timeout interval for a rating server. If the rating server times out a second time, this server is removed from server list. Minimum *timeout* value is 0 and has no upper limit.	R+B
as freeSession	Frees (deletes) all mail sessions.	R+B
as getServerList <y|n>	Sends a request for a server list manually.	R+B
as rtnct clear	Clears the record of non-routed emails.	R
as rtnct disp	Counts how many emails were not routed and records the reason for not routing.	R
as scoreTimeout <*timeout*>	Sets a timeout period for a query to a rating server for an antispam score. *timeout* value is 0-30 seconds.	R+B
as xtag <*tag*><*content*>	Sets a message (xtag) in the mail header. The tag depends on the mail application used. Examples are <X-Mailer> or <X-MimeOLE>. *tag* *content*	R+B

The following table shows a list of default values.

Table 10 as Default Values

VARIABLE	DEFAULT VALUE
asAction	1
antispam	disabled
failTolerance	120 seconds
scoreTimeout	7 seconds

3.2 Command Examples

Use this example to load the antispam module and configure it to filter email received from the WAN and addressed to a client on the LAN.

```
ras> as enable 1
Anti spam: enabled
ras> as dir WAN1 LAN on
From\To  lan  wan1 dmz  wan2 wlan vpn
=======================================
lan      off  off  off  off  off  off
wan1     on   off  off  off  off  off
dmz      off  off  off  off  off  off
wan2     off  off  off  off  off  off
wlan     off  off  off  off  off  off
vpn      off  off  off  off  off  off
ras>
```

4

Antivirus Commands

Use these commands to configure antivirus related settings on the ZyWALL.

4.1 Command Summary

The following table describes the values required for many antivirus (`av`) commands. Other values are discussed with the corresponding commands.

Table 11 av Command Input Values

LABEL	DESCRIPTION
protocol	Specifies a protocol. The options are `ftp|http|pop3|smtp`
interface	Specifies an interface. The options are `lan|wan1|dmz|wlan|vpn.`

The following section lists the commands for this feature.

.

Table 12 av Commands

COMMAND	DESCRIPTION	M
`av config decompress <on|off>`	Enables or disables zip file decompression on the fly to one level of decompression. TCP packet assembly checking also needs to be enabled to support this function. Use `av tune config l7...asm` to enable TCP packet assembly checking if is not already enabled.	R+B
`av config enable <on|off>`	Enables or disables the antivirus function.	R+B
`av config [`*`protocol`*`] active <on|off>`	Enables or disables the antivirus function for the specified protocol.	R+B
`av config [`*`protocol`*`] dir [`*`interface`*`][`*`interface`*`][on|off]`	Configures antivirus protection for the specified protocol based on the source and destination of traffic.	R+B
`av config [`*`protocol`*`] display`	Shows the antivirus setting for the specified protocol.	R+B
`av config httpScanAllMime <on|off>`	Enables or disables scanning of ASCII files transferred using HTTP, such as .txt, .html. By default, the ZyWALL scans MIME type files, for example, .doc, .ppt, .zip, .exe.	R+B
`av config overZipSession [0|1]`	Blocks (0) or forwards (1) a mail with an attached zip file when the maximum number of received zip files has been exceeded.	R+B
`av config pop3ScanAllMime <on|off>`	Enables or disables scanning of ASCII files transferred using POP3 (email), such as .txt, .html. By default, the ZyWALL scans MIME type files, for example, .doc, .ppt, .zip, .exe.	R+B

Table 12 av Commands (continued)

COMMAND	DESCRIPTION	M
`av config smtpScanAllMime <on|off>`	Enables or disables scanning of ASCII files transferred using SMTP (email), such as .txt, .html. By default, the ZyWALL scans MIME type files, for example,.doc, .ppt, .zip, .exe.	R+B
`av display`	Shows the antivirus settings.	R+B
`av load`	Loads the antivirus settings.	R+B
`av save`	Saves the antivirus settings.	R+B
`av signature load <`*`signature-id`*`>`	Loads the specified signature (so you can configure it). *`signature-id`*: Each intrusion signature has a unique identification number. This number may be searched at myZyXEL.com for more detailed information.	R+B
`av signature config active <on|off>`	Turns the signature you loaded on or off.	R+B
`av signature config alert <on|off>`	Enables or disables alerts for the signature you loaded.	R+B
`av signature config destroyFile <on|off>`	Enables or disables the destruction of files that match the virus signature you loaded.	R+B
`av signature config log <on|off>`	Enables or disables logs for packets that match the signature you loaded.	R+B
`av signature config sendWinMsg <on|off>`	Enables or disables a pop-up message in Windows notifying the detection of a file that matches the virus signature you loaded.	R+B
`av signature display`	Displays the currently loaded signature's settings.	R+B
`av signature reset`	Resets all of the antivirus signatures to their default settings.	R+B
`av signature save`	Saves your configuration changes for the signature you loaded.	R+B
`av tune config l4Icmpcjsum <on|off>`	Use the following `av tune config` commands to configure tune settings such as checksum checking and packet ordering for IDP/Anti-Virus/Anti-Spam protection. While these features improve security, there is a tradeoff in performance. Enables or disables ICMP checksum checking.	R+B
`av tune config l4Tcpcksum <on|off>`	Enables or disables TCP checksum checking.	R+B
`av tune config l4Tcpmssck <on|off>`	Enables or disables TCP MSS (Maximum Segment Size) checking.	R+B
`av tune config l4Tcpwindowck <on|off>`	Enables or disables TCP window checking.	R+B
`av tune config l4Udpcksum <on|off>`	Enables or disables UDP checksum checking.	R+B
`av tune config l7Ftpasm <on|off>`	Enables or disables TCP packet assembly checking for FTP traffic.	R+B
`av tune config l7Ftpdataasm <on|off>`	Enables or disables TCP packet assembly checking for FTPDATA.	R+B
`av tune config l7Httpasm <on|off>`	Enables or disables TCP packet assembly checking for HTTP.	R+B
`av tune config l7Otherasm <on|off>`	Enables or disables TCP packet assembly checking for other protocols.	R+B

Table 12 av Commands (continued)

COMMAND	DESCRIPTION	M
`av tune config l7Pop3asm <on|off>`	Enables or disables TCP packet assembly checking for POP3.	R+B
`av tune config l7Smtpasm <on|off>`	Enable or disables TCP packet assembly checking for SMTP.	R+B
`av tune display`	Displays the tune configuration.	R+B
`av tune load`	Loads the tune configuration.	R+B
`av tune save`	Saves the tune configuration.	R+B
`av update config autoupdate <on|off>`	Enables or disables the signature autoupdate.	R+B
`av update config dailyTime <00-23>`	Configures the signature update time of day.	R+B
`av update config method <1-3>`	Configures the signature update method. 1 : hourly 2 : daily 3 : weekly	R+B
`av update config weeklyDay <1-7>`	Configures which day of the week the signature is updated. 1 : sun 2 : mon 3 : tue 4 : wed 5 : thu 6 : fri 7 : sat	R+B
`av update config weeklyTime <00-23>`	Configures which hour of the day the signature is updated.	R+B
`av update display`	Shows the signature information and the update settings.	R+B
`av update load`	Loads the signature update setting.	R+B
`av update save`	Saves the signature update setting.	R+B
`av update start`	Starts the signature update.	R+B

The following table shows a list of default values.

Table 13 av Default Values

VARIABLE	DEFAULT VALUE
`decompress`	on
`av on or off`	off
`av` *`protocol`*	off
`av alert`	on
`av breakfile`	on
`log`	on
`sendmsg (popup)`	on
`overZipSession`	off
`ScanAllMime`	off
`checksum`	off

Table 13 av Default Values

VARIABLE	DEFAULT VALUE
`17...asm (packet order checking)`	on
`autoupdate`	off

4.2 Command Examples

This example loads the antivirus signature, enables antivirus protection, zip file decompression, and virus scanning on SMTP traffic from the LAN to the WAN.

```
ras> av load
ras> av config enable on
ras> av config decompress on
ras> av config smtp active on
ras> av config smtp dir lan wan1 on
From\To  lan  wan1 dmz  wlan vpn
=======================================
lan      off  on   off  off  off
wan1     off  off  off  off  off
dmz      off  off  off  off  off
wlan     off  off  off  off  off
vpn      off  off  off  off  off
ras> av save
```

5

Auxiliary (Dial Backup) Commands

Use these commands to configure dial backup (auxiliary) port settings on the ZyWALL.

5.1 Command Summary

The following table describes the values required for many dial backup commands. Other values are discussed with the corresponding commands.

Table 14 Dial Backup Command Input Values

LABEL	DESCRIPTION
aux-port	This identifies the channel (device) for dial backup. `aux0`: This is the dial backup port. `aux1`: This is the 3G WAN connection. This only applies to devices with a 3G WAN connection.

The following section lists the `aux` commands.

Table 15 Dial Backup Commands

COMMAND	DESCRIPTION	M
`aux atring <aux-port>`	Shows the AT command strings that the ZyWALL has sent to the WAN device and the responses.	R
`aux cdmamdm flag [1|0]`	1 allows the ZyWALL to dial a CDMA modem connected to the dial backup port.	R
`aux cnt clear <aux-port>`	Clears the auxiliary port's counter information.	R
`aux cnt disp <aux-port>`	Displays the auxiliary port's counter information.	R
`aux dial <aux-port> <phone-number>`	Has the ZyWALL dial the modem. Include a # symbol at the beginning of the phone number as required.	R
`aux disableDSRCheck`	The LG 340 wireless modem does not send a DSR when it is ready. Use this command with a LG 340 wireless modem to have the ZyWALL not check for a DSR signal.	R
`aux dqtest <aux-port>`	Sends the AT command to the WAN device	R
`aux drop <aux-port>`	Disconnects the auxiliary port's connection.	R
`aux enableDSRCheck`	Has the ZyWALL check for a DSR signal from the modem. Use this command if you have stopped using a LG 340 wireless modem and want to change to a regular modem (that sends a DSR when it is ready).	R
`aux init <aux-port>`	Initializes the auxiliary port's connection.	R

Table 15 Dial Backup Commands (continued)

COMMAND	DESCRIPTION	M
`aux mstatus` <*aux-port*>	Displays the status of the modem’s last call.	R
`aux mtype` <*aux-port*>	Displays the type of modem connected to the auxiliary port.	R
`aux netstat` <*aux-port*>	Displays upper layer packet information for the specified device.	R
`aux rate` <*aux-port*>	Displays the transmit and receive rates.	R
`aux signal` <*aux-port*>	Displays the auxiliary port’s signal.	R
`aux usrmdm flag [1|0]`	1 allows the ZyWALL to dial a US Robotics modem connected to the dial backup port.	R

5.2 Command Examples

This example displays upper layer packet information for the dial backup port.

```
as> aux netstat aux0
Name   :       aux0, Dev type  :    3, Chann id:    0

RX(pkt):          0, RX discard:    0, RX error:    0, RX(octet):          0
TX(pkt):          0, TX discard:    0, TX error:    0, TX(octet):          0
```

The following table describes the labels in this display.

Table 16 aux netstat aux0

LABEL	DESCRIPTION
Name	Name of the channel.
Dev type	The type of auxiliary device, there are several possibilities: 0: NONE 1: 56k modem 2: modems other than 56k 3: TA 4: X25_PAD 5: MultiProtocol over AAL5 6: PPP over Ethernet, RFC-2516 7: PPTP 8: 3G modem
Chann id	The number of the channel that the device is using.
RX (pkt)	Received packets.
TX (pkt	Transmitted packets.
RX discard	Received octets the ZyWALL discarded.
TX discard	Transmitted octets the ZyWALL discarded.
RX error	Received errored frames.
TX error	Transmitted errored frames.
RX(octet)	Received errored octets.
TX(octet)	Transmitted errored octets.

This example displays the dial backup port’s transmit and receive rates.

```
ras> aux rate aux0
 No. TX(byte) Rx(byte)  TX Rate   RX Rate   TX Queue
==== ======== ======== ========= ========= ==========
   1        0        0         0         0          0
   2        0        0         0         0          0
   3        0        0         0         0          0
   4        0        0         0         0          0
   5        0        0         0         0          0
   6        0        0         0         0          0
   7        0        0         0         0          0
   8        0        0         0         0          0
   9        0        0         0         0          0
  10        0        0         0         0          0
  11        0        0         0         0          0
  12        0        0         0         0          0
  13        0        0         0         0          0
  14        0        0         0         0          0
  15        0        0         0         0          0
  16        0        0         0         0          0
  17        0        0         0         0          0
  18        0        0         0         0          0
  19        0        0         0         0          0
  20        0        0         0         0          0
```

The following table describes the labels in this display.

Table 17 aux rate aux0

LABEL	DESCRIPTION
No.	The entry in the rate statistics.
TX (byte)	Transmitted bytes.
Rx (byte	Received bytes.
TX Rate	Transmission rate.
RX Rate	Received rate
TX Queue	Number of packets waiting to be transmitted.

This example displays details about the dial backup port’s signal.

```
ras> aux signal aux0

 DTR: OFF DSR: OFF RTS: OFF CTS: OFF DCD: OFF
```

The following table describes the labels in this display.

Table 18 aux rate aux0

LABEL	DESCRIPTION
DTR	Data Terminal Ready: The signal the ZyWALL sends to the modem to indicate the ZyWALL is ready to receive data.
DSR	Data Set Ready: The signal the modem sends to the ZyWALL to indicate the modem is ready to receive data.

Table 18 aux rate aux0 (continued)

LABEL	DESCRIPTION
RTS	Request to Send: The signal the ZyWALL sends to the modem to have the modem prepare to receive data.
CTS	Clear to Send: The signal the modem sends to the ZyWALL to acknowledge the ZyWALL and allow the ZyWALL to transmit data.
DCD	Data Carrier Detect: The signal the modem sends to the ZyWALL when the modem has a connection with the remote device.

This example shows the AT command strings that the ZyWALL has sent to the modem connected to the dial backup port and the responses.

```
ras> aux atring aux0
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

94b13960: 02 0d 0c 00 be af 00 00 00 00 08 00 61 74 68 0d     ............ath.
94b13970: 0d 0a 4f 4b 0d 0a 61 74 26 66 73 30 3d 30 0d 0d     ..OK..at&fs0=0..
94b13980: 0a 4f 4b 0d 0a 61 74 64 30 2c 34 30 35 30 38 38     .OK..atd0,405088
94b13990: 38 38 0d 0d 0a 42 55 53 59 0d 0a 61 74 64 30 2c     88...BUSY..atd0,
94b139a0: 34 30 35 30 38 38 38 38 0d 0d 0a 52 49 4e 47 49     40508888...RINGI
94b139b0: 4e 47 0d 0a 0d 0a 42 55 53 59 0d 0a 61 74 64 30     NG....BUSY..atd0
94b139c0: 2c 34 30 35 30 38 38 38 38 0d 0d 0a 43 4f 4e 4e     ,40508888...CONN
94b139d0: 45 43 54 20 31 31 35 32 30 30 2f 56 2e 33 34 20      ECT 115200/V.34
94b139e0: 31 36 38 30 30 2f 56 34 32 62 0d 0d 0a 4e 4f 20      16800/V42b...NO
94b139f0: 43 41 52 52 49 45 52 0d 0a 61 74 68 0d 0d 0a 4f     CARRIER..ath...O
94b13a00: 4b 0d 61 74 68 0d 0d 0a 4f 4b 0d 0a 61 74 26 66     K.ath...OK..at&f
94b13a10: 73 30 3d 30 0d 0d 0a 4f 4b 0d 0a 61 74 64 30 2c     s0=0...OK..atd0,
94b13a20: 34 30 35 30 38 38 38 38 0d 0d 0a 43 4f 4e 4e 45     40508888...CONNE
94b13a30: 43 54 20 31 31 35 32 30 30 2f 56 2e 33 34 20 31     CT 115200/V.34 1
94b13a40: 34 34 30 30 2f 56 34 32 62 0d 0d 0a 4e 4f 20 43     4400/V42b...NO C
94b13a50: 41 52 52 49 45 52 0d 0a 61 74 68 0d 0d 0a 4f 4b     ARRIER..ath...OK
94b13a60: 0d 61 74 68 0d 0d 0a 4f 4b 0d 0a 61 74 26 66 73     .ath...OK..at&fs
94b13a70: 30 3d 30 0d 0d 0a 4f 4b 0d 0a 61 74 64 30 2c 34     0=0...OK..atd0,4
94b13a80: 30 35 30 38 38 38 38 0d 0d 0a 43 4f 4e 4e 45 43     0508888...CONNEC
94b13a90: 54 20 31 31 35 32 30 30 2f 56 2e 33 34 20 20 39     T 115200/V.34  9
94b13aa0: 36 30 30 2f 56 34 32 62 0d 00 00 00 00 00 00 00     600/V42b........
```

Bandwidth Management Commands

Use these commands to configure bandwidth management (BWM) settings on the ZyWALL.

6.1 Command Summary

The following table describes the values required for many commands. Other values are discussed with the corresponding commands.

Table 19 Bm Class Command Input Values

LABEL	DESCRIPTION
<interface>	This is an interface name including lan, wan/wan1, dmz, wan2, wlan.
name *<class-name>*	This is a class name. Enter a descriptive name of up to 20 alphanumeric characters, including spaces.
class-number	This is a class number. Each class for each interface has an unique number. The number format is "xx.xx.xx.xx...xx" and the range of xx is from 01 to 98. Each ".xx" is a subclass. And the length of "xx.xx.xx.xx..." is the depth of this class. Different model supports different class depth.

The following section lists the commands for this feature.

Table 20 Bm Interface Commands

COMMAND	DESCRIPTION	M
bm interface <*interface*> <enable|disable> [bandwidth <*bps*>] [prr|wrr] [efficient]	Enables or disables BWM for traffic going out of the specified interface. *bps*: The unit is bps and its minimum is 2000. You can alternatively type “K” or “k” to specify kbps while “M” or “m” to specify Mbps. If you do not specify the bandwidth, the default value is 100 Mbps. prr|wrr: Sets the queuing mechanism to fairness-based (WRR) or priority-based (PRR). efficient: Turns on the Maximum Bandwidth Usage option.	R+B
bm class <*interface*> <add|del|mod> <*class-number*> [bandwidth <*bps*>] [name <*class_name*>] [priority <*x*>] [borrow <on|off>]	Adds, deletes, or modifies a class for the specified interface with the specified bandwidth. You can also configure other options including name, priority, or bandwidth borrowing. add|del|mod: Adds, deletes, or modifies the class. When you delete a class, it also deletes its sub-classes. bandwidth <*bps*>: Uses this command when you add or modify a class. The unit is bps and its minimum is 2000. You can alternatively type “K” or “k” to specify kbps while “M” or “m” to specify Mbps. name <*class_name*>: The name is for your information. priority <*x*>: Sets the class priority ranging from 0 (the lowest) to 7 (the highest). borrow <on|off>: The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa.	R+B
bm monitor <*interface*> [*class-number*]	Displays the bandwidth usage of the specified interface or its class. The first time you use the command turns it on; the second time turns it off, and so on.	R+B
bm filter <*interface*> add <*class-number*> [service <*type*>] <single|range|subnet> <*dst-start-ip*> [*dst-end-ip*] <*dport*> <*dportend*> <single|range|subnet> <*src-start-ip*> [*src-end-ip*] <*sport*> <*sportend*> <*protocol*>	Adds a filter for the specified class. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. Use 0 to not include items in the filter. service <*type*>: This is service type including ftp, sip, or h323 in lower cases. Following are the settings for filter rule's destination address. single|range|subnet *dst-start-ip* *dst-end-ip* *dport* *dportend* Following are the settings for filter rule's source address. single|range|subnet *src-start-ip* *src-end-ip* *sport* *sportend* *dst-end-ip*, *src-end-ip*: When you configure a single address, you don't need to specify these options. When you configure a range address, these are network ending IP address. When you configure a subnet, these are subnet mask, ex. 255.255.255.0.	R+B

Table 20 Bm Interface Commands (continued)

COMMAND	DESCRIPTION	M
`bm filter <interface> del <class-number>`	Deletes a filter for the specified class.	R+B
`bm show <interface|class|filter|statistics> <interface>`	Displays interface setting, class, filter setting, or statistics for the specified interface.	R+B
`bm moveFilter <interface> <from> <to>`	Changes the BWM filter order. *from*, *to*: A filter index number.	R+B
`bm config [load|save|clear]`	Loads, saves, clears BWM configuration from/to the non-volatile memory.	R+B
`bm vpnTraffic <on|off>`	Sets the BWM classifier to use the outer IP header of encrypted VPN traffic (when sets on) or the IP header of unencrypted VPN traffic (when sets off).	R+B
`bm packetBased <on|off>`	Sets the BWM classifier operation to be session based or packet based. By default, it is session based.	R+B

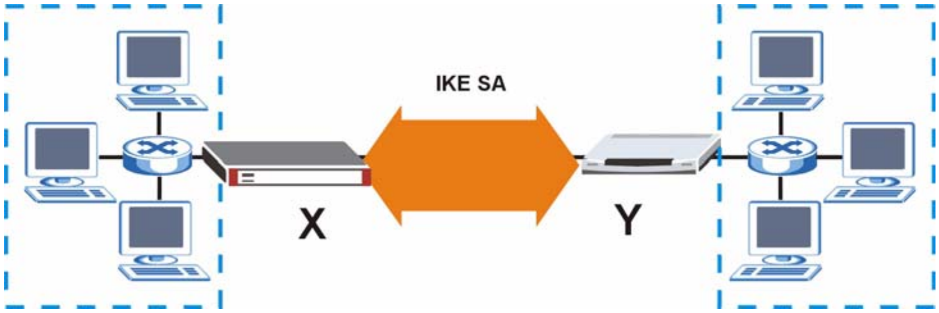
6.2 Managing the Bandwidth of VPN Traffic

Syntax:

```
bm vpnTraffic [on|off]
```

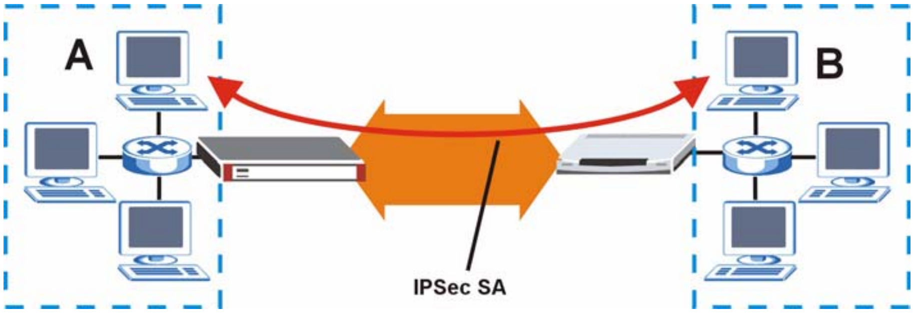
By default the ZyWALL uses the outer source and destination IP addresses of encrypted VPN packets in managing the bandwidth of the VPN traffic (when using "on" with this command). These are the IP addresses of the ZyWALL and the remote IPSec router. The following figure shows an example of this. The ZyWALL uses the IP addresses of the ZyWALL (X in the figure) and the remote IPSec router (Y) to manage the bandwidth of the VPN traffic.

Figure 1 Managing the Bandwidth of an IPSec tunnel



Use on with this command to be able to create a single bandwidth management group that includes all of the phase 2 IPSec SAs that are connecting through the same remote IPSec router. With this setting the bandwidth management applies to ESP or AH packets so you can only specify IP addresses in the BWM filter settings.

Figure 2 Managing the Bandwidth of VPN traffic between hosts



How you configure this command affects how you can implement bandwidth management as follows.

- Leave this command set to `off` to be able to create bandwidth management groups for individual unencrypted VPN traffic that are connecting through the same remote IPSec router. With this setting you can also specify the type of traffic either using the service list (like SIP or FTP) or by specifying port numbers in BWM filter settings.
- Use `off` with this command to set the ZyWALL uses the source and destination IP addresses of unencrypted VPN packets in managing the bandwidth of the VPN traffic. This means that it looks at the IP address of the computer that sent the packets and the IP address of the computer to which it is sending the packets. The following figure shows an example of this. The ZyWALL uses the IP addresses of computers A and B to manage the bandwidth of the VPN traffic.

6.3 Command Examples

This example displays the LAN interface's BWM settings and then configures the LAN interface using bandwidth 10,000 bps and the priority-based queuing method.

```
ras> bm show interface lan
===============================================================================
Interface : LAN         [ Enabled ]

        bandwidth =    100M (bps)
        allocated bandwidth =      0 (bps)
        MTU = 1500 (byte)
===============================================================================
ras> bm interface iface lan enable bandwidth 10000 prr
```

This example adds one LAN class using following settings.

- Class number: 1
- Bandwidth: 5,000,000 bps
- Class Name: LAN-class1

```
ras> bm config load
ras> bm class lan add 1 bandwidth 5M name LAN-class1
ras> bm config save
```

This example modifies one existing LAN class using following settings and displays what we configured then.

- Class number: 1
- Bandwidth: 50,000,000 bps
- Priority:2
- Enable the Borrowing option: Yes

```
ras> bm config load
ras> bm class lan mod 1 bandwidth 50M
ras> bm config save
ras> bm show class lan
===============================================================================
Class: 0        Name: Root Class
        depth: 0        priority: 0     filter setting: No
        queue: 0/30
        borrow class: No
        parent class: No

        total bandwidth:        100M (bps)
        allocated bandwidth:     50M (bps)
===============================================================================
Class: 1        Name: LAN-class1
        depth: 1        priority: 2     filter setting: No
        queue: 0/30
        borrow class: 1
        parent class: 0 (Root Class)

        total bandwidth:         50M (bps)
        allocated bandwidth:      0 (bps)
===============================================================================
Class: 99       Name: Default Class
        depth: 1        priority: 0     filter setting: Yes
        queue: 0/30
        borrow class: 0
        parent class: 0 (Root Class)

        total bandwidth:         50M (bps)
        allocated bandwidth:      0 (bps)
===============================================================================
```

This example adds one LAN subclass using following settings and displays what we configured then.

- Class number: 1.5 (subclass 5 under the class 1)
- Bandwidth: 600,000 bps.
- Class Name: LAN-FTP
- Priority: 3

- Enable the Borrowing option: No

```
ras> bm config load
ras> bm class lan add 1.5 bandwidth 600k name LAN-FTP priority 3 borrow off
ras> bm config save
ras> bm show class lan
================================================================================
Class: 0        Name: Root Class
        depth: 0        priority: 0     filter setting: No
        queue: 0/30
        borrow class: No
        parent class: No

        total bandwidth:        100M (bps)
        allocated bandwidth:     50M (bps)
================================================================================
Class: 1        Name: LAN-class1
        depth: 1        priority: 2     filter setting: No
        queue: 0/30
        borrow class: 1
        parent class: 0 (Root Class)

        total bandwidth:         50M (bps)
        allocated bandwidth:    600K (bps)
================================================================================
Class: 1.5      Name: LAN-FTP
        depth: 2        priority: 3     filter setting: No
        queue: 0/30
        borrow class: No
        parent class: 1 (LAN-class1)

        total bandwidth:        600K (bps)
        allocated bandwidth:      0 (bps)
================================================================================
Class: 99       Name: Default Class
        depth: 1        priority: 0     filter setting: Yes
        queue: 0/30
        borrow class: 0
        parent class: 0 (Root Class)

        total bandwidth:         50M (bps)
        allocated bandwidth:      0 (bps)
================================================================================
```

This example modifies one existing LAN subclass using following settings.

- Class number: 1.5
- Bandwidth: 800,000 bps.
- Enable the Borrowing option: Yes

```
ras> bm config load
ras> bm class lan mod 1.5 bandwidth 800k borrow on
ras> bm config save
ras>
```

This example adds a filter on the LAN subclass using following settings.

- Class number: 1.5
- Destination address: Single, 10.1.1.20, FTP ports from 20 to 21.
- Source address: Subnet, 192.168.1.0/24, any port.
- Protocol: any protocol.

```
ras> bm config load
ras> bm filter lan add 1.5 single 10.1.1.20 20 21 subnet 192.168.1.0
255.255.255.0 0 0 0
Filter setting is done.
ras> bm config save
ras> bm show filter lan
===============================================================================
Class 1.5       Name: LAN-FTP
        Protocol: 0
        Destination type: SINGLE
        Destination address: 10.1.1.20/10.1.1.20
        Destination port: 20~21
        Source type: SUBNET
        Source address: 192.168.1.0/255.255.255.0
        Source port: 0~0
===============================================================================
Class 99        Name: Default Class
        Protocol: 0
        Destination type: SINGLE
        Destination address: 0.0.0.0/0.0.0.0
        Destination port: 0~0
        Source type: SINGLE
        Source address: 0.0.0.0/0.0.0.0
        Source port: 0~0
===============================================================================
ras>
```

This example monitors the runtime situation for all WAN classes.

Each interface has one root class (0) and one default class (99). In this example, you can see only one user-defined class (1). The root class (0) displays total traffic amount for the WAN interface. The current bandwidth usage matching to the class 1 rule is 500Kb. For traffic that doesn't match any user-defined class rule, it is counted in the default class (99).

```
ras> bm monitor wan
WAN - 0: 500Kb 1: 500Kb 99: 0b
WAN - 0: 500Kb 1: 500Kb 99: 0b
WAN - 0: 500Kb 1: 500Kb 99: 0b
WAN - 0: 900Kb 1: 500Kb 99: 400b
WAN - 0: 900Kb 1: 500Kb 99: 400b
```

7

Bridge Commands

Use these commands to configure bridge settings on the ZyWALL.

7.1 Command Summary

The following table describes the values required for many bridge commands. Other values are discussed with the corresponding commands.

Table 21 Bridge Command Input Values

LABEL	DESCRIPTION
interface	This identifies an interface. 1: WAN1 2: WAN2 3: LAN 4: Wireless card 5: DMZ 6: WLAN (ports in WLAN port role)

The following section lists the `bridge` commands.

Table 22 Bridge Commands

COMMAND	DESCRIPTION	M
`bridge block <ipx|poe|ip|arp|bpdu|unknow> <on|off>`	Blocks IPX, PoE, IP, ARP, BPDU, and/or unknown Ethernet frames from passing through in bridge mode.	B
`bridge cnt clear`	Resets the bridging statistics counter.	R+B
`bridge cnt disp`	Displays the bridging statistics table.	R+B
`bridge iface active <yes|no>`	Sets the ZyWALL to bridge mode or router mode.	R+B
`bridge iface address [`*ip-address*`]`	Sets the bridge mode management IP address.	B
`bridge iface display`	Displays the bridge mode interface settings.	B
`bridge iface dns1 [`*ip-address*`]`	Sets the bridge mode first system DNS server IP address.	B
`bridge iface dns2 [`*ip-address*`]`	Sets the bridge mode second system DNS server IP address.	B
`bridge iface dns3 [`*ip-address*`]`	Sets the bridge mode third system DNS server IP address.	B
`bridge iface gateway [`*gateway-ip*`]`	Sets the bridge mode default gateway.	B
`bridge iface mask [`*mask*`]`	Sets the bridge mode network mask.	B
`bridge rstp bridge disable`	Turns off RSTP.	B

Table 22 Bridge Commands (continued)

COMMAND	DESCRIPTION	M
`bridge rstp bridge enable`	Turns on RSTP (Rapid Spanning Tree Protocol).	B
`bridge rstp bridge forwardDelay [`*`forwarding-delay`*`]`	Sets the RSTP forwarding delay (4~30). This is the number of seconds a bridge remains in the listening and learning port states. The default is 15 seconds.	B
`bridge rstp bridge helloTime [`*`hello-time`*`]`	Sets the RSTP hello time (1~10) in seconds the root bridge waits before sending a hello packet.	B
`bridge rstp bridge maxAge [`*`max-age`*`]`	Sets the RSTP max age (6~40). This is how many seconds a bridge waits to get a Hello BPDU from the root bridge.	B
`bridge rstp bridge priority [`*`priority`*`]`	Sets the ZyWALL's RSTP bridge priority (0~61440). The lower the number, the higher the priority. Bridge priority determines the root bridge, which in turn determines Hello Time, Max Age and Forward Delay.	B
`bridge rstp bridge version <STP:0|RSTP:2>`	Sets the ZyWALL to use STP or RSTP.	B
`bridge rstp disp`	Displays RSTP information.	B
`bridge rstp port disable <`*`interface`*`>`	Turns off RSTP on the specified port.	B
`bridge rstp port edgePort <`*`interface`*`> <True:1|False:0>`	Sets the specified port to be an edge or non-edge port.	B
`bridge rstp port enable <`*`interface`*`>`	Turns on RSTP on the specified port.	B
`bridge rstp port mcheck <`*`interface`*`>`	Sets migrate check on this port	B
`bridge rstp port p2pLink <`*`interface`*`> <Auto:2|True:1|False:0>`	Sets a point to point link on the specified port.	B
`bridge rstp port pathCost <`*`interface`*`> [`*`path-cost`*`]`	Sets the RSTP path cost on the specified port.	B
`bridge rstp port priority <`*`interface`*`> [`*`priority`*`]`	Sets the RSTP priority on the specified port.	B
`bridge rstp state`	Displays general RSTP status information.	B
`bridge rstp trace`	Turns on RSTP debug/trace messages.	B
`bridge stat clear`	Resets the bridging packet statistics counter.	R+B
`bridge stat disp`	Displays the bridging packet statistics table.	R+B

7.2 Command Examples

This example enables RSTP on the ZyWALL; enables RSTP on the WAN and displays the RSTP settings.

```
ras> bridge rstp bridge enable
ras> bridge rstp port enable 3
ras> bridge rstp disp
Bridge Info:
  (a)BridgeID:                  8000-0000aa100586
  (b)TimeSinceTopoChange:       745
  (c)TopoChangeCount:           0
  (d)TopoChange:                0
  (e)DesignatedRoot:            8000-0000aa100586
  (f)RootPathCost:              0
  (g)RootPort:                  0x0000
  (h)MaxAge:                    20      (seconds)
  (i)HelloTime:                 2       (seconds)
  (j)ForwardDelay:              15      (seconds)
  (k)BridgeMaxAge:              20      (seconds)
  (l)BridgeHelloTime:           2       (seconds)
  (m)BridgeForwardDelay:        15      (seconds)
  (n)TransmissionLimit:         3
  (o)ForceVersion:              2

Port [03] Info:
  (a)Uptime:                    746     (seconds)
  (b)State:                     FORWARDING
  (c)PortID:                    0x8003
  (d)PathCost:                  250
  (e)DesignatedRoot:            8000-0000aa100586
  (f)DesignatedCost:            0
  (g)DesignatedBridge:          8000-0000aa100586
  (h)DesignatedPort:            0x8003
  (i)TopoChangeAck:             False
  (j)adminEdgePort:             True
  (k)operEdgePort:              True
  (m)MAC_Operational:           True
  (n)adminPointToPointMAC:        (o)operPointToPointMAC:       True
  rx_cfg_bpdu[   0]     rx_tcn_bpdu[   0]       rx_rstp_bpdu[   0]
```

8

Certificates Commands

Use these commands to configure certificates.

8.1 Command Summary

The following table describes the values required for many `certificates` commands. Other values are discussed with the corresponding commands.

Table 23 Certificates Commands Input Values

LABEL	DESCRIPTION
auth-key	Specifies the certificate's key for user authentication. If the key contains spaces, put it in quotes. To leave it blank, type "".
ca-address	The IP address or domain name of the CA (Certification Authority) server.
ca-cert	The name of the CA certificate.
ip-address[:*port*]	Specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389.
key-length	The length of the key to use in creating a certificate or certificate request. Valid options are 512, 768, 1024, 1536 and 2048 bits.
login:*pswd*	The login name and password for the directory server, if required. The format is "login:*password*".
name	The identifying name of a certificate or certification request. Use up to 31 characters to identify a certificate. You may use any character (not including spaces).
proxyurl	The address and port of an optional HTTP proxy to use.
server-name	A descriptive name for a directory server. Use up to 31 ASCII characters (spaces are not permitted).
subject	A certificate's subject name and alternative name. Both are required. The format is "subject-name-dn;{ip,dns,email}=value". Example 1: "CN=ZyWALL,OU=CPE SW2,O=ZyXEL,C=TW;ip=172.21.177.79" Example 2: "CN=ZyWALL,O=ZyXEL,C=TW;dns=www.zyxel.com" Example 3: "CN=ZyWALL,O=ZyXEL,C=TW;email=dummy@zyxel.com.tw" If the name contains spaces, put it in quotes.
timeout	The verification timeout value in seconds (optional). The default timeout value is 20 seconds.
url	The location of a certificate to be imported.

The following section lists the `certificates` commands.

Table 24 Certificates Commands

COMMAND	DESCRIPTION	M
`certificates ca_trusted crl_issuer <name> [on|off]`	Specifies whether or not the specified CA issues a CRL. `on|off`: specifies whether or not the CA issues CRL. If `[on|off]` is not specified, the current CRL issuer status of the CA displays.	R+B
`certificates ca_trusted delete <name>`	Removes the specified trusted CA certificate.	R+B
`certificates ca_trusted export <name>`	Exports the specified PEM-encoded certificate to your CLI session's window for you to copy and paste.	R+B
`certificates ca_trusted http_import <url> <name> [proxyurl]`	Imports the specified certificate file from the specified remote web server as a trusted CA. The certificate file must be in one of the following formats: 1) Binary X.509, 2) PEM-encoded X.509, 3) Binary PKCS#7, and 4) PEM-encoded PKCS#7.	R+B
`certificates ca_trusted import <name>`	Imports the specified PEM-encoded CA certificate from your CLI session. After you enter the command, copy and paste the PEM-encoded certificate into your CLI session window. With some terminal emulation software you may need to move your mouse around to get the transfer going.	R+B
`certificates ca_trusted list`	Displays all trusted CA certificate names and their basic information.	R+B
`certificates ca_trusted rename <old-name> <new-name>`	Renames the specified trusted CA certificate.	R+B
`certificates ca_trusted verify <name> [timeout]`	Has the ZyWALL verify the certification path of the specified trusted CA certificate.	R+B
`certificates ca_trusted view <name>`	Displays details about the specified trusted CA certificate.	R+B
`certificates cert_manager reinit`	Re-initializes the certificate manager.	R+B
`certificates dir_service add <server-name> <ip-address[:port]> [login:pswd]`	Adds a new directory server entry.	R+B
`certificates dir_service delete <server-name>`	Removes the specified directory server entry.	R+B
`certificates dir_service edit <server-name> <ip-address[:port]> [login:pswd]`	Edits the specified directory server entry.	R+B
`certificates dir_service list`	Displays all directory server entry names and their basic information.	R+B
`certificates dir_service rename <old-server-name> <new-server-name>`	Renames the specified directory server entry.	R+B
`certificates dir_service view <server-name>`	Displays details about the specified directory server entry.	R+B
`certificates my_cert create scep_enroll <name> <ca-address> <ca-cert><ra-sign> <ra-encr> <auth key> <subject> [key length]`	Creates a certificate request and enrolls for a certificate immediately online using SCEP protocol. `ra-sign`: specifies the name of the RA (Registration Authority) signing certificate. If it is not required, type "" to leave it blank. `ra-encr`: specifies the name of the RA encryption certificate. If it is not required, type "" to leave it blank .	R+B

Table 24 Certificates Commands (continued)

COMMAND	DESCRIPTION	M
`certificates my_cert create cmp_enroll <name> <ca-address> <ca-cert> <auth-key> <subject> [key-length]`	Creates a certificate request and enroll for a certificate immediately online using CMP protocol.	R+B
`certificates my_cert create request <name> <subject> [key-length]`	Creates a certificate request and saves it on the ZyWALL for later manual enrollment.	R+B
`certificates my_cert create self_signed <name> <subject> <key-length> [validity-period]`	Creates a self-signed local host certificate. *key-length*: specifies the key size. Valid options are 0, 512, 768, 1024, 1536 and 2048 bits. 0 applies the default value of 1024. *validity-period*: specifies the validity period in years. Valid range is 1~30. The default is 3.	R+B
`certificates my_cert def_selfsigned [name]`	Sets the specified self-signed certificate as the default self-signed certificate. If you do not specify a name, the name of the current self-signed certificate displays.	R+B
`certificates my_cert delete <name>`	Removes the specified local host certificate.	R+B
`certificates my_cert export <name>`	Exports the PEM-encoded certificate to your CLI session window for you to copy and paste.	R+B
`certificates my_cert http_import <url> <name> [proxy-url]`	Imports the specified certificate file from the specified remote web server as the device's own certificate. The certificate file must be in one of the following formats: 1) Binary X.509, 2) PEM-encoded X.509, 3) Binary PKCS#7, and 4) PEM-encoded PKCS#7. A certification request corresponding to the imported certificate must already exist. The certification request is automatically deleted after the importation.	R+B
`certificates my_cert import [name]`	Imports the PEM-encoded certificate from your CLI session. A corresponding certification request must already exist on the ZyWALL. The certification request is automatically deleted after the importation. The name is optional, if you do not specify one, the certificate adopts the name of the certification request. After you enter the command, copy and paste the PEM-encoded certificate into your CLI session window. With some terminal emulation software you may need to move your mouse around to get the transfer going.	R+B
`certificates my_cert list`	Displays all my certificate names and basic information.	R+B
`certificates my_cert poll_req <name>`	Queries an SCEP server about a certification request that is pending in an SCEP server's queue.	R+B
`certificates my_cert rename <old-name> <new-name>`	Renames the specified my certificate.	R+B
`certificates my_cert replace_factory`	Creates a certificate using your device MAC address that is specific to this device. The factory default certificate is a common default certificate for all ZyWALL models.	R+B
`certificates my_cert verify <name> [timeout]`	Has the ZyWALL verify the certification path of the specified local host certificate.	R+B
`certificates my_cert view <name>`	Displays information about the specified local host certificate.	R+B
`certificates remote_trusted delete <name>`	Removes the specified trusted remote host certificate.	R+B

Table 24 Certificates Commands (continued)

COMMAND	DESCRIPTION	M
certificates remote_trusted export <*name*>	Exports the PEM-encoded certificate to your CLI session's window for you to copy and paste.	R+B
certificates remote_trusted http_import <*url*> <*name*> [*proxy-url*]	Imports the specified certificate file from the specified remote web server as the device's trusted remote host. The certificate file must be in one of the following formats: 1) Binary X.509, 2) PEM-encoded X.509, 3) Binary PKCS#7, and 4) PEM-encoded PKCS#7. *proxy-url*: Specifies the location of the certificate to be imported.	R+B
certificates remote_trusted import <*name*>	Imports the specified PEM-encoded remote host certificate from your CLI session. After you enter the command, copy and paste the PEM-encoded certificate into your CLI session window. With some terminal emulation software you may need to move your mouse around to get the transfer going.	R+B
certificates remote_trusted list	Displays all trusted remote host certificate names and their basic information.	R+B
certificates remote_trusted rename <*old-name*> <*new-name*>	Renames the specified trusted remote host certificate.	R+B
certificates remote_trusted verify <*name*> [*timeout*]	Has the ZyWALL verify the certification path of the specified trusted remote host certificate.	R+B
certificates remote_trusted view <*name*>	Displays information about the specified trusted remote host certificate.	R+B

8.2 Command Examples

This example creates and displays a self signed certificate named "test" with a subject alternative common name of "cert-test" organization of "my-company", country of "TW", and IP 172.16.2.2. It uses a 512 bit key and is valid for 5 years.

```
ras> certificates my_cert create self_signed test "CN=cert-test,O=my-
company,C=TW;ip=172.16.2.2" 512 5
The self-signed certificate has been successfully generated.
ras> certificates my_cert list
PKI Storage Space in Use: 2%
[      Certificate Name       ]  Type [ Subject Name ] [ Issuer Name ] From [To]
auto_generated_self_signed_cert *SELF CN=ZyWALL 70 ... CN=ZyWALL 70... 2000 2030
test                             SELF CN=cert-test,... CN=cert-test... 2007 2012
--------------------------------------------------------------------------------
Total number of certificates: 2
Legends: NYV - Not Yet Valid, EXPD - Expired, EXPG - Expiring, CERT -
Certificate, REQ - Certification Request, SELF - Self-signed Certificate, *SELF
- Default Self-signed Certificate
```

This example displays the certificate that the ZyWALL is using as the default self-signed certificate. Then it has the ZyWALL use the self signed certificate named “test” as the default self-signed certificate.

```
ras> certificates my_cert def_self_signed
The default self-signed certificate: auto_generated_self_signed_cert
ras> certificates my_cert def_self_signed test
Would you like to make "test" as the default self-signed certificate? (y/n):y
ras> certificates my_cert def_self_signed
The default self-signed certificate: test
```

This example exports the self signed certificate named “test”. After the certificate displays on the screen, copy and paste it into a text editor (like Notepad) and save it as a .crt or .cer file.

```
ras> certificates my_cert export test
-----BEGIN CERTIFICATE-----
MIIBlzCCAUGgAwIBAgIEOlptnzANBgkqhkiG9w0BAQUFADA2MQswCQYDVQQGEwJU
VzETMBEGA1UEChMKbXktY29tcGFueTESMBAGA1UEAxMJY2VydC10ZXN0MB4XDTAx
MDEwODAxNDcxMVoXDTA2MDEwOTAxNDcxMVowNjELMAkGA1UEBhMCVFcxEzARBgNV
BAoTCm15LWNvbXBhbnkxEjAQBgNVBAMTCWNlcnQtdGVzdDBcMA0GCSqGSIb3DQEB
AQUAA0sAMEgCQQDmnKh6ZZ5xaPukE4+djC6bu0Uyjf5aQ/QysD+Udv8xF0L/DpT1
c3xnu8hkp/RCFS3/fK6ALiLsoMCOUmqg5bdDAgMBAAGjNzA1MA4GA1UdDwEBAAQE
AwICpDAPBgNVHREECDAGhwSsFyXLMBIGA1UdEwEBAAQIMAYBAf8CAQEwDQYJKoZI
hvcNAQEFBQADQQC9hq27VCDTu6L2JsDgU8jXwYghDDKXzPR5PZ4/oryX5PFILrtr
rNLh2eTCExnyyEggaRhJ0B63Ucam7hG4k5xW
-----END CERTIFICATE-----
```

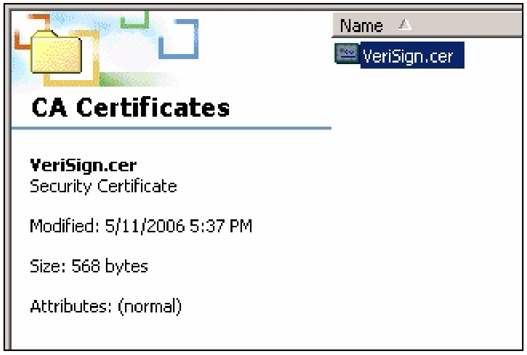
This example imports a VeriSign certificate as a trusted CA. The CA certificate has to be PEM-encoded. Refer to Section 8.2.1 on page 59 for how to save a certificate in PEM-encoded format.

```
ras> certificates ca_trusted import VeriSign
Please paste the PEM-encoded certificate onto the screen.
Press Ctrl+D when finished or Ctrl+C to cancel.
Note: 9600 bps console port speed guarantees minimum transmission error
rate.
-----END CERTIFICATE-----rTJXwT4OPjr0l91X817/OWOgHz8UA==ZHuO3ABc
```

8.2.1 Saving Certificates as PEM-encoded Format

Do the following to save a certificate in PEM-encoded format.

1 In Windows Explorer, locate and double-click the (non PEM-encoded) certificate file.



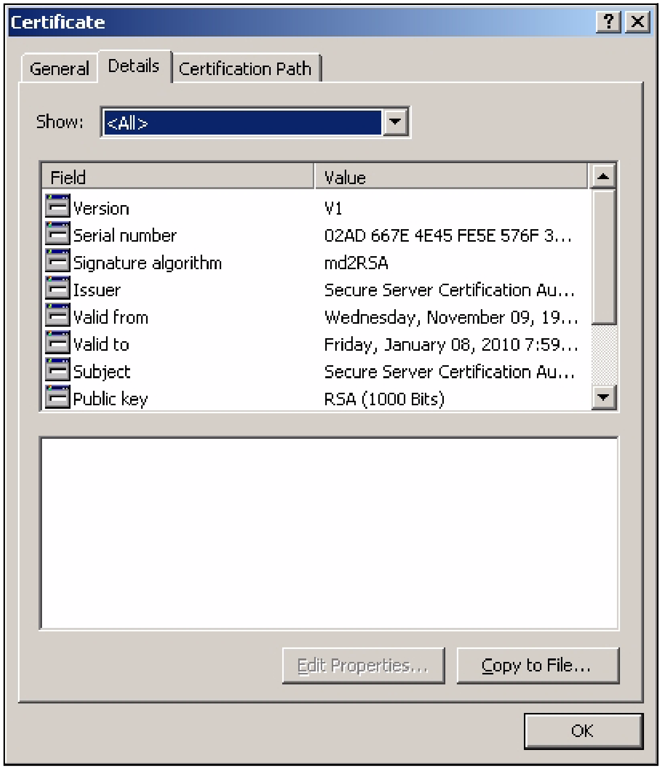
VeriSign.cer
Security Certificate

Modified: 5/11/2006 5:37 PM

Size: 568 bytes

Attributes: (normal)

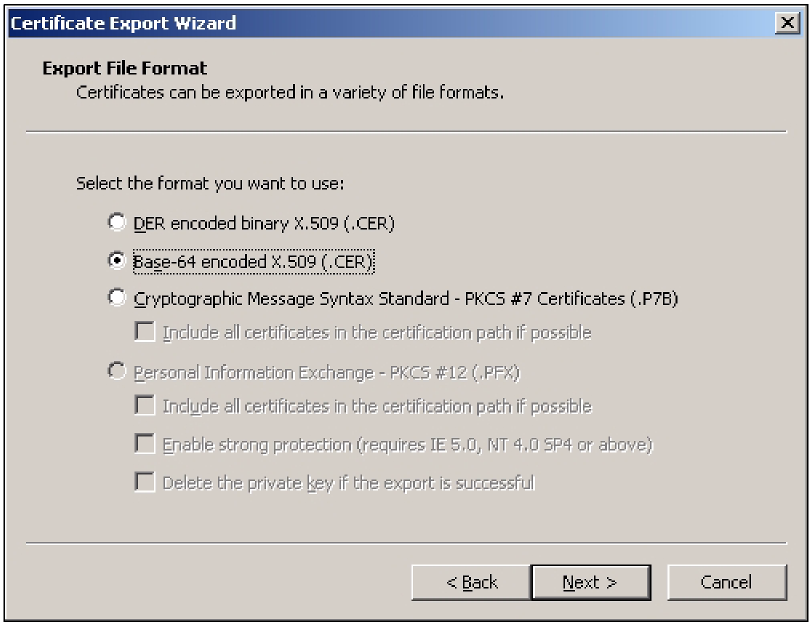
2 Click **Details** and **Copy to File**.



Show: <All>

Field	Value
Version	V1
Serial number	02AD 667E 4E45 FE5E 576F 3...
Signature algorithm	md2RSA
Issuer	Secure Server Certification Au...
Valid from	Wednesday, November 09, 19...
Valid to	Friday, January 08, 2010 7:59...
Subject	Secure Server Certification Au...
Public key	RSA (1000 Bits)

3 Click **Next** in the welcome screen. Select **Base-64 encoded X.509 (.CER)**.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

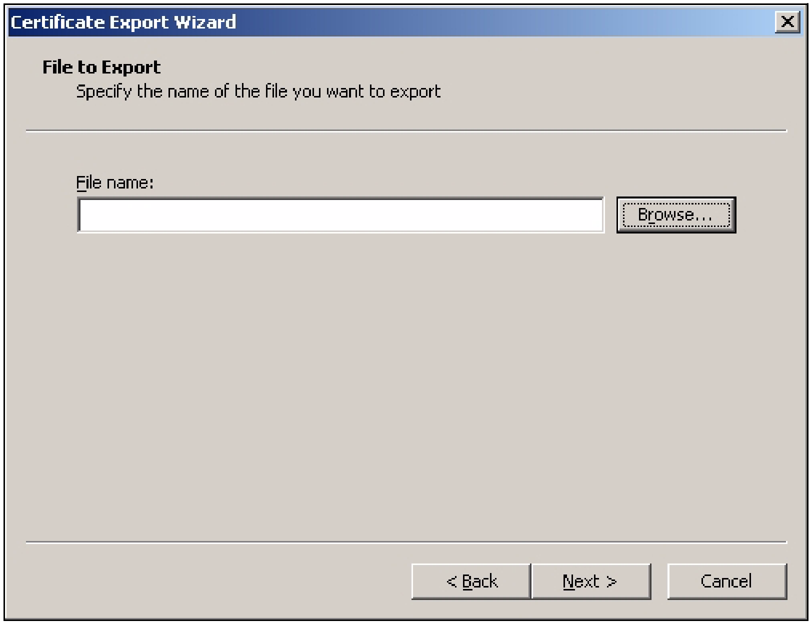
○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

4 Type a file name (or browse for one).



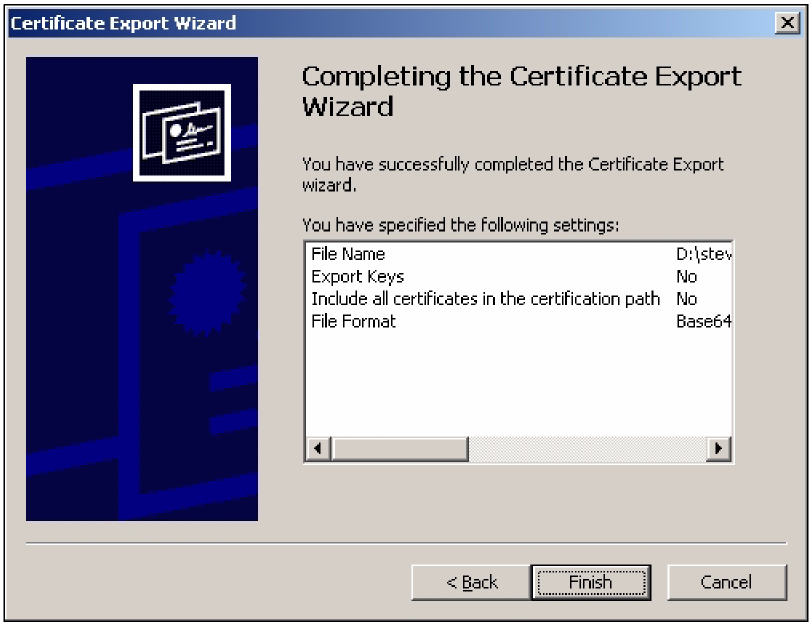
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

5 Click **Finish**.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	D:\stev
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64

6 Open the newly created file in a text editor (like Notepad) to be able to copy and paste the certificate into your CLI session.

9

CNM Agent Commands

Use these commands to configure CNM agent settings on the ZyWALL.

9.1 Command Summary

The following section lists the commands for this feature.

Table 25 CNM Commands

COMMAND	DESCRIPTION	M
`cnm active [0:disable|1:enable]`	Enables or disables the CNM service on the ZyWALL. After enabled, the ZyWALL communicates with the CNM server through ZyWALL's WAN.	R+B
`cnm sgid`	Displays the unique ID received from the CNM server after the ZyWALL registered successfully.	R+B
`cnm managerIp`	Displays the CNM server's IP address.	R+B
`cnm debug [0:disable|1:enable]`	Controls whether the debugging information is displayed on the console. You must change the baud rate to 115200 bps before enabling the CNM debug mode.	R+B
`cnm reset`	Resets the CNM service to the initial status on the ZyWALL. The ZyWALL will register itself to the CNM server again if the service is enabled.	R+B
`cnm encry [none|des|3des]` [*key*]	Displays or sets the encryption mode and key. The encryption key is 8 characters when the encryption mode is set to "DES". The encryption key is 24 characters when the encryption mode is set to "3DES".	R+B
`cnm keepalive <10~90>`	Sets how often (in seconds) the ZyWALL sends a keepalive packet to inform the CNM server of its existence.	R+B
`cnm version`	Displays the CNM agent version.	R+B
`cnm alarmqueue display`	Displays the alert messages waiting to be sent to the CNM server.	R+B
`cnm alarmqueue send`	Sends all alert messages in the queue to the CNM server immediately and clears the queue.	R+B

9.2 Command Examples

This example displays the CNM agent version on the ZyWALL.

```
ras> cnm version
cnm version: 2.0.2(AGZ.1)b1
```

This example configures the CNM settings and activates the service on the ZyWALL using the following settings.

- CNM server IP address: 10.1.1.252
- Encryption mode: DES
- Encryption key: 12345678
- How often to send a keepalive packet to the CNM server: every 60 seconds

```
ras> cnm managerIp 10.1.1.252
managerIp 10.1.1.252
ras> cnm encry des 12345678
cnm encry des 12345678
ras> cnm keepalive 60
cnm keepalive 60ras> cnm active 1
cnm active 1
Last Register Time: 0-0-0 0:0:0
```

This example displays the CNM debug messages. It's useful for monitoring register or keepalive packets the ZyWALL sends and receives to and from the CNM server.

```
ras> cnm debug 1
cnm debug 1 <0:Disable 1:Enable> CNM debug messges can only be printed at 115200
 baud rate.
ras>
agentIpAddr: 10.1.1.252
CNM protocol version = 1
sendSgmpRegisterRequest sessionID = [0]
sgmpAgentRx iface_p=b04088 cnt=1
sgmpRxEventProcess opType 1
procAgentRegister
SessionID is modified by Vantage to [0]
received SGMP_T_REGISTER:SGMP_C_RESPONSE
Error tUnit=4096
sendSgmpRegisterAck ackCode=9
procAgentRetrieve event SGMP_EVENT_REGISTER_RESP
sendSgmpRetrieveStoreRequest opType=2
sgmpd state SGMP_STATE_REGISTERING
sgmpAgentRx iface_p=b04088 cnt=1
sgmpRxEventProcess opType 2
procAgentRetrieve, agentState = 1
SessionID is modified by Vantage to [0]
received SGMP_T_RETRIEVE:SGMP_C_RESPONSE
sendSgmpRetrieveStoreAck opType=2 ackCode=9
procAgentRetrieve event SGMP_EVENT_RETRIEVE_RESP
sgmpd state SGMP_STATE_RETRIEVE_INIT
 event: SGMP_EVENT_RETRIEVE_SUCCESS
sendRetrieveStoreSucc opType=2 opCode=3
sendSgmpRegisterSuccess
sgmpd state SGMP_STATE_ACTIVE
 No Alarms Exist!
sgmpAgentRx iface_p=b04088 cnt=1
sgmpRxEventProcess opType 9
SessionID is modified by Vantage to [478043139]
tUint = 4110, Amount_Item = 1, nUnit = 1
procInquireData FORWARD COMPATIBILITY
 Device (1b55) unsupport CNM Forward Compatibility!!
 Fail to send Forward Comp Information to CNM.
call sendSgmpInquireSuccess
sendSgmpInquireSuccess opType=9 opCode=4 sessionID =[1909254747]
Send SGMP KA Trap IP=10.1.1.252, life=0, interval=90 (secs)
 No Alarms Exist!
Send SGMP KA Trap IP=10.1.1.252, life=90, interval=90 (secs)
 No Alarms Exist!
```

10

Configuration Commands

Use these commands to configure your configuration settings on the ZyWALL. Many of these commands are also available in the web configurator.

10.1 Command Summary

The following table describes the values required for many `config` commands. Other values are discussed with the corresponding commands.

Table 26 config Command Input Values

LABEL	DESCRIPTION
day	Specifies which day. Options are `sunday|monday|tuesday|wednesday|thursday|friday|saturday.`
entry#	Specifies which custom service (from 1~100). A custom service allows you to configure a port for specific applications such as P2P applications. The available sub-fields are: name <*string*> range <*start-port*><*end-port*> ip-protocol <`icmp|tcp|udp|tcp/udp|user-defined`> user-defined-ip <1~255> icmp-type <0~255> icmp-code <0~255>
mask	Describes a subnet mask in dotted decimal notation.
non-zero-number	A non-zero number used to indicate a black or white filter rule is enabled.
rule#	Specifies which rule from in a set. A rule is used to describe an action to be taken when a packet matches the rule description. The number of rules available depends on the product. See Section 10.3.2 on page 81 for a detailed description of the parameters.
rule-action	Specifies the action to take when a rule applies to a packet. The options are `permit|drop|reject.`
send-email-policy	Specifies when to send an e-mail. Options are full|hourly|daily|weekly|none.
set#	Specifies which set. A set is a named set of rules and actions applying to packets with a specified source and destination interface. Set numbers go from 1~255. See Section 10.3.1 on page 77 for a detailed description of the parameters.

Table 26 config Command Input Values

LABEL	DESCRIPTION
string, e-mail	< 31 ASCII characters.
timeout	This is measured in seconds between 0~4294967295 seconds. Editing, deleting or inserting these values has no effect. To configure these *timeout* values use `tos` commands, as these are global settings.

The following section lists the commands for this feature.

Table 27 `config` Command Summary

COMMAND	DESCRIPTION	M
`config cli`	Displays the features you can configure with the `config` command.	R+B
`config delete anti-spam blackRule`	Removes the antispam blacklist. The blacklist is a list of IP addresses of known spammers to be blocked.	R+B
`config delete anti-spam whiteRule`	Removes the antispam whitelist. The whitelist is a list of IP addresses known to be safe.	R+B
`config delete custom-service <entry#>`	Deletes the specified custom service entry.	R+B
`config delete custom-service <entry#> icmp-code`	Deletes the ICMP code. This field is optional for ICMP. The code and type of an ICMP packet together indicate the purpose of the packet.	R+B
`config delete custom-service <entry#> icmp-type`	Deletes the ICMP type.	R+B
`config delete custom-service <entry#> ip-protocol`	Deletes the IP protocol for a selected custom service.	R+B
`config delete custom-service <entry#> name`	Deletes the name of the selected custom service.	R+B
`config delete custom-service <entry#> range`	Deletes the port range setting for the custom service.	R+B
`config delete custom-service <entry#> user-defined-ip`	Deletes the IP protocol setting for the custom service.	R+B
`config delete firewall active`	Deletes the active setting in the firewall rule configuration.	R+B
`config delete firewall attack block`	Deletes the block setting in the firewall rule configuration.	R+B
`config delete firewall attack block-minute`	Deletes the block attack in minutes setting in the firewall rule configuration.	R+B
`config delete firewall attack max-incomplete-high`	Deletes the setting for DOS (Denial of Service) detection based on the maximum number of sessions allowed.	R+B
`config delete firewall attack max-incomplete-low`	When the ZyWALL detects a DOS attack it begins to delete half-open sessions until it reaches a specified number of half-open sessions. This commands deletes this set number.	R+B
`config delete firewall attack minute-high`	Deletes the setting for DOS detection based on the maximum number of sessions allowed per minute.	R+B
`config delete firewall attack minute-low`	When the ZyWALL detects a DOS attack it begins to delete half-open sessions until it reaches a specified number of half-open sessions per minute. This commands deletes this set number.	R+B

Table 27 `config` Command Summary (continued)

COMMAND	DESCRIPTION	M
`config delete firewall attack send-alert`	Deletes the setting for whether an alert should be sent on registering an attack.	R+B
`config delete firewall attack tcp-max-incomplete`	Deletes the setting for DOS detection based on the maximum number of sessions allowed with the same destination host address.	R+B
`config delete firewall e-mail`	Removes all settings for e-mailing the firewall log.	R+B
`config delete firewall e-mail day`	Deletes the setting for which day the firewall log e-mail is sent.	R+B
`config delete firewall e-mail email-to`	Deletes the setting for where the e-mail is sent to.	R+B
`config delete firewall e-mail hour`	Deletes the setting for which hour the e-mail is sent.	R+B
`config delete firewall e-mail mail-server`	Deletes the setting for which e-mail server is used to send the e-mail.	R+B
`config delete firewall e-mail minute`	Deletes the setting for which minute the e-mail is sent at.	R+B
`config delete firewall e-mail policy`	Deletes the setting for the schedule for when the e-mail is sent.	R+B
`config delete firewall e-mail return-addr`	Deletes the setting for the return address for the e-mail log.	R+B
`config delete firewall e-mail subject`	Deletes the setting for the subject of the e-mail log.	R+B
`config delete firewall set <set#>`	Removes the specified set of rules applying to traffic from a given interface to another.	R+B
`config delete firewall set <set#> connection-timeout`	Deletes the setting for the connection time out for traffic to which this set applies. This command has no effect on firewall settings. To configure *`timeout`* values use `tos` commands	R+B
`config delete firewall set <set#> default-action`	Deletes the setting for the default action for traffic to which this set applies.	R+B
`config delete firewall set <set#> fin-wait-timeout`	Deletes the setting for the wait time for FIN when concluding a TCP session before it is terminated. This command has no effect on firewall settings. To configure *`timeout`* values use `tos` commands	R+B
`config delete firewall set <set#> icmp-timeout`	Deletes the setting for the timeout for an idle ICMP session before it is terminated. This command has no effect on firewall settings. To configure *`timeout`* values use `tos` commands	R+B
`config delete firewall set <set#> log`	Deletes the log of traffic to which this set applies.	R+B
`config delete firewall set <set#> name`	Deletes the name of a set.	R+B
`config delete firewall set <set#> rule <rule#>`	Removes a specified rule in a set from the firewall configuration.	R+B
`config delete firewall set <set#> rule <rule#> action`	Deletes whether a packet is permitted, dropped or rejected when it matches this rule.	R+B
`config delete firewall set <set#> rule <rule#> active`	Deletes whether a rule is enabled or not.	R+B

Table 27 config Command Summary (continued)

COMMAND	DESCRIPTION	M
config delete firewall set <*set#*> rule <*rule#*> alert	Deletes whether or not there is notification of a DoS attack or a violation of the alert settings.	R+B
config delete firewall set <*set#*> rule <*rule#*> custom-icmp	Deletes the desired ICMP custom service.	R+B
config delete firewall set <*set#*> rule <*rule#*> custom-ip	Deletes the desired user defined IP Protocol custom service.	R+B
config delete firewall set <*set#*> rule <*rule#*> destaddr-range	Deletes the IP address range setting in a rule applying to a packet with a destination IP address which falls within the specified range.	R+B
config delete firewall set <*set#*> rule <*rule#*> destaddr-single	Deletes the IP address setting for a rule applying to a packet with the destination IP address.	R+B
config delete firewall set <*set#*> rule <*rule#*> destaddr-subnet	Deletes the IP address and subnet mask settings for a rule applying to a packet with the destination IP address and subnet mask.	R+B
config delete firewall set <*set#*> rule <*rule#*> destport-custom	Deletes the desired TCP/UDP custom port name.	R+B
config delete firewall set <*set#*> rule <*rule#*> log	Deletes a log for a rule when the packet matches the rule.	R+B
config delete firewall set <*set#*> rule <*rule#*> name	Deletes the rule name.	R+B
config delete firewall set <*set#*> rule <*rule#*> protocol	Deletes the protocol number for a rule.	R+B
config delete firewall set <*set#*> rule <*rule#*> srcaddr-range	Deletes the IP address range for a rule applying to a packet with a source IP address that falls within a specified range.	R+B
config delete firewall set <*set#*> rule <*rule#*> srcaddr-single	Deletes the IP address setting in a rule applying to a packet with a specified source IP address.	R+B
config delete firewall set <*set#*> rule <*rule#*> srcaddr-subnet	Deletes the IP address and subnet mask setting in a rule applying to a packet with a specified source IP address and subnet mask.	R+B
config delete firewall set <*set#*> rule <*rule#*> tcp destport-any	Deletes the rule applying to a TCP packet with any destination port.	R+B
config delete firewall set <*set#*> rule <*rule#*> tcp destport-range	Deletes the port setting for a rule applying to a TCP packet with a destination port falling within the specified range.	R+B
config delete firewall set <*set#*> rule <*rule#*> tcp destport-single	Deletes the port setting for a rule applying to a TCP packet with the specified destination port.	R+B
config delete firewall set <set#> rule <rule#> udp destport-any	Deletes the rule applying to a UDP packet with any destination port.	R+B
config delete firewall set <*set#*> rule <*rule#*> udp destport-range	Deletes the port range setting for a rule applying to a UDP packet with a destination port falling within the specified range.	R+B
config delete firewall set <*set#*> tcp-idle-timeout	Deletes the timeout for an idle TCP session before it is terminated. This command has no effect on firewall settings. To configure *timeout* values use tos commands.	R+B
config delete firewall set <*set#*> udp-idle-timeout	Deletes the timeout for an idle UDP session before it is terminated. This command has no effect on firewall settings. To configure *timeout* values use tos commands.	R+B

Table 27 `config` Command Summary (continued)

COMMAND	DESCRIPTION	M
`config display anti-spam`	Displays all the antispam settings.	R+B
`config display custom-service`	Displays all configured custom services. See Table 26 on page 67 for a list of custom-service parameters.	R+B
`config display custom-service <entry#>`	Displays the custom service for the entry number given (1~100).	R+B
`config display firewall`	Displays all the firewall settings for all firewall sets. Available firewall sub-commands are: • active • e-mail • attack • set	R+B
`config display firewall attack`	Displays all the attack alert settings. These are: send-alert block minute-high minute-low max-incomplete-high max-incomplete-low tcp-max-incomplete	R+B
`config display firewall buffer`	Displays the firewall ACL (Access Control List) buffer size. The size is product dependent and cannot be changed.	R+B
`config display firewall e-mail`	Displays all the firewall e-mail log settings. These are: mail-server return-addr email-to subject policy	R+B
`config display firewall set <set#>`	Displays current entries of a set. See Table 26 on page 67 for a list of set parameters.	R+B
`config display firewall set <set#> rule <rule#>`	Displays the current entries of a rule in a set. See Table 26 on page 67 for a list of rule parameters.	R+B
`config edit anti-spam action <0|1>`	Sets the action for spam: 0: add a tag 1: discard mail.	R+B
`config edit anti-spam blackRule <0|1>`	Enables (1) or disables (0) the antispam blacklist filter.	R+B
`config edit anti-spam externDB <0|1>`	Enables (1) or disables (0) the external database query feature. Queries are sent to an external database to check whether an e-mail is likely to be spam.	R+B
`config edit anti-spam markString <spam-tag>`	Sets the Spam tag string (< 16 chars). This tag is added to the subject of spam mail.	R+B
`config edit anti-spam phishingString <phishing-tag>`	Sets the phishing tag string (< 16 chars). This tag is added to the subject of spam mail.	R+B
`config edit anti-spam query <0|1>`	Sets the action for mail which receives a “no spam” score. 0: add a tag 1: discard mail	R+B
`config edit anti-spam queryString <no-spam-score-tag>`	Sets the tag string (< 16 chars) for mail which receives a “no spam” score. This tag is added to the subject of spam mail.	R+B

Table 27 `config` Command Summary (continued)

COMMAND	DESCRIPTION	M
`config edit anti-spam rule <rule#> email <1:whitelist|2:blacklist> active <0:disable|non-zero-number:enable> data <e-mail>`	Sets an antispam rule based on the e-mail address on a black or white list filter. *e-mail*: should be < 64 chars.	R+B
`config edit anti-spam rule <rule#> ip <1:whitelist|2:blacklist> active <0:disable|non-zero-number:enable> address <ip-address> netmask <mask>`	Sets an antispam rule based on the IP address and subnet mask on a black or white list filter.	R+B
`config edit anti-spam rule <rule#> mime <1:whitelist|2:blacklist> active <0:disable|non-zero-number:enable> header <mime-header> value <mime-value>`	Sets an antispam rules based on the MIME type on a black or white list filter. <*mime-header*>: This indicates the MIME type. <*mime-value*>: This is a user-defined tag attached to emails.	R+B
`config edit anti-spam switch <0|1>`	Enables (1) or disables (0) the antispam function.	R+B
`config edit anti-spam threshold <threshold>`	Sets the spam score threshold. If the spam score is higher than this threshold, this mail is judged as spam mail. <*threshold*>: A number from 1~100.	R+B
`config edit anti-spam whiteRule <0|1>`	Enables (1) or disables (0) the antispam whitelist filter.	R+B
`config edit custom-service <entry#> icmp-code <0~255>`	Configures the ICMP code. This field is optional for ICMP. The code and type of an ICMP packet together indicate the purpose of the packet. Use `config edit custom-service <entry#> icmp-type` to configure the ICMP type first.	R+B
`config edit custom-service <entry#> icmp-type <0~255>`	Configures the ICMP type.	R+B
`config edit custom-service <entry#> ip-protocol <icmp|tcp|udp|tcp/udp|user-defined>`	Configures the IP protocol for a selected custom-service.	R+B
`config edit custom-service <entry#> name <string>`	Sets the name of the selected custom-service.	R+B
`config edit custom-service <entry#> range <start-port><endport>`	When the IP protocol is set to TCP and/or UDP, this command configures the port range for a specified custom-service entry. For single port configuration, the start port is equal to the end port.	R+B
`config edit custom-service <entry#> user-defined-ip <1~255>`	When the IP protocol is set to “user-defined”, this command configures the user defined IP protocol.	R+B
`config edit firewall active <yes|no>`	Activates or deactivates the saved firewall settings.	R+B
`config edit firewall attack block <yes|no>`	Select “yes” to block traffic when it exceeds the tcp-max-incomplete threshold. Select “no” to delete the oldest half-open session when the number of half-opened sessions exceeds the tcp-max-incomplete threshold.	R+B
`config edit firewall attack block-minute <0~255>`	Sets the time a session is blocked once an attack is detected. This command is only valid when '`block`' is set to “yes”. The unit is minute.	R+B

Table 27 config Command Summary (continued)

COMMAND	DESCRIPTION	M
config edit firewall attack max-incomplete-high <0~255>	Sets the threshold for DOS detection based on the maximum number of half-opened sessions allowed. Half-opened sessions will be deleted after this level is reached to bring the number down to max-incomplete-low.	R+B
config edit firewall attack max-incomplete-low <0~255>	Sets the level at which the firewall will stop deleting half-opened sessions once a DOS attack has been detected.	R+B
config edit firewall attack minute-high <0~255>	Sets the threshold to start deleting the old half-opened sessions based on the number of half-opened sessions per minute.	R+B
config edit firewall attack minute-low <0~255>	Sets the threshold to stop deleting the old half-opened session once a DOS attack has been detected and sufficient half-opened sessions have been deleted. This threshold is based on the number of half-opened sessions per minute.	R+B
config edit firewall attack send-alert <yes|no>	This activates or deactivates notification by e-mail of DoS attacks detected by the firewall.	R+B
config edit firewall attack tcp-max-incomplete <0~255>	Sets the threshold for DoS detection based on the maximum number of sessions allowed with the same destination host address.	R+B
config edit firewall e-mail day <*day*>	Sets the day to send the log when the e-mail policy is set to weekly.	R+B
config edit firewall e-mail e-mail-to <*e-mail*>	Sets the mail address to send the log.	R+B
config edit firewall e-mail hour <0~23>	Sets the hour to send the log when the e-mail policy is set to daily or weekly.	R+B
config edit firewall e-mail mail-server <*ip-address*>	Sets the IP address of the mail server's used to send the alert.	R+B
config edit firewall e-mail minute <0~59>	Sets the minute to send to log when the e-mail policy is set to daily or weekly.	R+B
config edit firewall e-mail policy <*send-email-policy*>	Sets the policy for when the firewall log is e-mailed.	R+B
config edit firewall e-mail return-addr <*e-mail*>	Sets the mail address for returning an e-mail alert.	R+B
config edit firewall e-mail subject <*mail-subject*>	Sets the e-mail subject.	R+B
config edit firewall set <set#> connection-timeout <*timeout*>	Sets the connection timeout for traffic to which a rule in the set applies. This command has no effect on firewall settings. To configure *timeout* values use tos commands.	R+B
config edit firewall set <set#> default-action <*rule-action*>	Sets the default action for traffic for which the set applies.	R+B
config edit firewall set <set#> fin-wait-timeout <*timeout*>	Sets the wait time for FIN when concluding a TCP session before it is terminated. This command has no effect on firewall settings. To configure *timeout* values use tos commands.	R+B
config edit firewall set <set#> icmp-timeout <*timeout*>	Sets the timeout for an idle ICMP session before it is terminated. This command has no effect on firewall settings. To configure *timeout* values use tos commands.	R+B

Table 27 config Command Summary (continued)

COMMAND	DESCRIPTION	M
config edit firewall set <*set#*> log <yes|no>	Edits whether a log of sessions for which the set applies is sent.	R+B
config edit firewall set <*set#*> name <*string*>	Edits the name for a set.	R+B
config edit firewall set <*set#*> rule <*rule#*> action <*rule-action*>	Edits whether a packet is permitted, dropped or rejected when it matches this rule.	R+B
config edit firewall set <*set#*> rule <*rule#*> active <yes|no>	Edits whether a rule is enabled or not.	R+B
config edit firewall set <*set#*> rule <*rule#*> alert <yes|no>	Activates or deactivates notification of a DoS attack or if there is a violation of any alert settings. When a DoS attack is detected the function will send an e-mail to the SMTP destination address and log an alert.	R+B
config edit firewall set <*set#*> rule <*rule#*> custom-icmp <*string*>	Sets the desired ICMP custom service. 1. You must first configure a ICMP service name using config edit custom-service <*entry#*> name <*string*>. 2. Then use config edit custom-service <*entry#*> ip-protocol icmp to set the protocol to ICMP. 3. Then use config edit custom-service <*entry#*> icmp-type to specify the ICMP type. 4. Then use config edit custom-service <*entry#*> icmp-code to specify the ICMP code. 5. After you save it you can add the custom-service to a firewall rule.	R+B
config edit firewall set <*set#*> rule <*rule#*> custom-ip <*string*>	Sets the desired user defined IP Protocol custom service. 1. You must first configure an IP protocol name using config edit custom-service <*entry#*> name <*string*>. 2. Then use config edit custom-service <*entry#*> ip-protocol user-defined-ip to enable setting the user-defined IP protocol. 3. You must use config edit custom-service <*entry#*> user-defined-ip <0~255> to set the IP protocol. 4. After you save it you can add the custom-service to a firewall rule.	R+B
config edit firewall set <*set#*> rule <*rule#*> destaddr-range <*start-ip*><*end-ip*>	Edits the rule to apply to a packet with a destination IP address which falls within the specified range.	R+B
config edit firewall set <*set#*> rule <*rule#*> destaddr-single <*ip-address*>	Edits the rule to apply to a packet with the destination IP address.	R+B
config edit firewall set <*set#*> rule <*rule#*> destaddr-subnet <*ip-address*> <*mask*>	Edits the rule to apply to a packet with the destination IP address and subnet mask.	R+B

Table 27 `config` Command Summary (continued)

COMMAND	DESCRIPTION	M
`config edit firewall set <set#> rule <rule#> destport-custom <string>`	Sets the desired TCP/UDP custom port name. 1. You must first configure a TCP/UDP service name using `config edit custom-service <entry#> name <string>`. 2. Then specify the IP Protocol using `config edit custom-service <entry#> ip-protocol`. The options are TCP, UDP or TCP/UDP. 3. Use `config edit custom-service <entry#> range` to set the port range(s) of the custom service. 4. After you save it you can add the custom-service to a firewall rule.	R+B
`config edit firewall set <set#> rule <rule#> log <none|match>`	Sends a log for a rule when the packet matches the rule.	R+B
`config edit firewall set <set#> rule <rule#> name <string>`	Edits the rule name.	R+B
`config edit firewall set <set#> rule <rule#> protocol <0~255>`	Edits the protocol number for a rule.	R+B
`config edit firewall set <set#> rule <rule#> srcaddr-range <start-ip><end-ip>`	Edits the rule to apply to a packet with a source IP address that falls within the specified range.	R+B
`config edit firewall set <set#> rule <rule#> srcaddr-single <ip-address>`	Edits the rule to apply to a packet with the specified source IP address.	R+B
`config edit firewall set <set#> rule <rule#> srcaddr-subnet <ip-address> <mask>`	Edits the rule to apply to a packet with any source IP address and subnet mask.	R+B
`config edit firewall set <set#> rule <rule#> tcp destport-any`	Edits the rule to apply to a TCP packet with any destination port. When using “?” with this command the system crashes.	R+B
`config edit firewall set <set#> rule <rule#> tcp destport-range <start-port><endport>`	Edits the rule to apply to a TCP packet with a destination port falling within the specified range. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers.	R+B
`config edit firewall set <set#> rule <rule#> tcp destport-single <port>`	Edits the rule to apply to a TCP packet with the specified destination port.	R+B
`config edit firewall set <set#> rule <rule#> udp destport-any`	Edits the rule to apply to a UDP packet with any destination port.	R+B
`config edit firewall set <set#> rule <rule#> udp destport-range <start-port><endport>`	Edits the rule to apply to a UDP packet with a destination port falling within the specified range. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers.	R+B
`config edit firewall set <set#> rule <rule#> udp destport-single <port>`	Edits the rule to apply to a UDP packet with the specified destination port.	R+B
`config edit firewall set <set#> tcp-idle-timeout <timeout>`	Edits the timeout for an idle TCP session before it is terminated. This command has no effect on firewall settings. To configure *`timeout`* values use `tos` commands.	R+B

Table 27 `config` Command Summary (continued)

COMMAND	DESCRIPTION	M
`config edit firewall set <set#> udp-idle-timeout <timeout>`	Edits the timeout for an idle UDP session before it is terminated. This command has no effect on firewall settings. To configure *`timeout`* values use `tos` commands.	R+B
`config insert firewall set <set#> rule <rule#>`	Inserts s new rule into a set. Use `config edit` commands to edit the rule and set subfields.	R+B
`config retrieve anti-spam`	Retrieves the current saved anti-spam settings.	R+B
`config retrieve custom-service <entry#>`	Retrieves the custom service entry specified by <*`entry#`*>.	R+B
`config retrieve firewall`	Retrieves current saved firewall settings.	R+B
`config save all`	Saves users' configurations into flash memory.	R+B
`config save anti-spam`	Saves the current antispam settings.	R+B
`config save custom-service <entry#>`	Saves the custom service entry specified by <*`entry#`*>.	R+B
`config save firewall`	Saves the current firewall settings.	R+B

10.2 Default Values

The following table shows a list of default values.

Table 28 config Default Values

VARIABLE	DEFAULT VALUE
`ACL set name:`	"ACL Default Set"
`anti-spam action <0|1>`	1
`anti-spam blackRule <0|1>`	0
`anti-spam markString <spam-tag>`	"SPAM"
`anti-spam phishingString <phishing-tag>`	"PHISHING"
`anti-spam query <0|1>`	0
`anti-spam switch <0|1>`	0
`anti-spam threshold <threshold>`	90
`anti-spam whiteRule <0|1>`	0
`connection-timeout`	30 seconds
`fin-wait-timeout`	60 seconds
`firewall active <yes|no>`	yes
`firewall attack block <yes|no>`	no
`firewall attack block-minute <0~255>`	10
`firewall attack max-incomplete-high <0~255>`	100
`firewall attack max-incomplete-low <0~255>`	80
`firewall attack minute-high <0~255>`	100
`firewall attack minute-low <0~255>`	80
`firewall attack send-alert <yes|no>`	no

Table 28 config Default Values

VARIABLE	DEFAULT VALUE
`firewall attack tcp-mac-incomplete <0~255>`	30
`firewall e-mail policy`	none
`icmp-timeout`	60 seconds
`tcp-idle-timeout`	3600 seconds
`udp-idle-timeout`	60 seconds

10.3 Command Examples

10.3.1 Firewall Example

Type the following commands to setup a firewall rule in WAN to WAN direction, with source IP = 1.1.1.1 and destination IP = 2.2.2.2. The configured service is SSH(TCP:22), logging is enabled, and the default action taken when a packet matches a rule is to permit the packet. Save your settings and then display them for checking.

```
config insert firewall set 8 rule 1
config edit firewall set 8 rule 1 srcaddr-single 1.1.1.1
config edit firewall set 8 rule 1 destaddr-single 2.2.2.2
config edit firewall set 8 rule 1 tcp destport-single 22
config edit firewall set 8 rule 1 log match
config edit firewall set 8 rule 1 action permit
config edit firewall set 8 rule 1 name SSH
ras> config display firewall set 8
ACL set number: 8(WAN1 to WAN1/ZyWALL)
   ACL set name: Cmz-Rules
   ACL set number of rules: 1
   ACL set default action: drop
   ACL pnc enable: no
   ACL log enable: no
   ACL logone enable: no
   ACL set timeout values:
   ICMP idle timeout (s): 60
   UDP idle timeout (s): 60
   TCP connection timeout (s): 30
   TCP FIN-wait timeout (s): 60
   TCP idle timeout (s): 3600
Free space remaining in ACL buffer: 161160
ras> config display set 8 rule 1
ACL rule number: 1
   ACL rule active: yes
   ACL rule action: permit
   ACL rule protocol:
   ACL rule log: match
   ACL rule alert: no
   Source Single IP address: 1.1.1.1
   Destination Single IP address: 2.2.2.2
   TCP destination port number(s): 22
   ACL rule name: SSH
ras> config save firewall
```

The following table describes the fields displayed using the `config display set` command in the example above.

Table 29 config display set

LABEL	DESCRIPTION
`ACL set number`	Shows the index number of this set and the interfaces it applies to. See
`ACL set name`	Shows the name of this set.
`ACL set number of rules`	Shows the number of rules in this set.
`ACL set default action`	Shows the default action when a packet matches a rule in the set. The options are: `permit|drop|reject.`
`ACL pnc enable`	Shows whether the pnc service is enabled. This service is currently not available.
`ACL log enable`	Shows whether the log is enabled or not.
`ACL logone enable`	Shows whether logone is enabled or not. This function is currently not available.
`ICMP idle timeout(s)`	Shows the timeout for an idle ICMP session before it is terminated.
`UDP idle timeout(s)`	Shows the timeout for an idle UDP session before it is terminated.
`TCP connection timeout(s)`	Shows the connection timeout for traffic to which a rule in the set applies.
`TCP FIN-wait timeout(s)`	Shows the wait time for FIN when concluding a TCP session before it is terminated.
`TCP idle timeout(s)`	Shows the timeout for an idle TCP session before it is terminated.

The following table describes the fields displayed using the `config display set <`*`index`*`> rule` command in the example above, as well as other related fields that may appear when configuring a rule using this command.

Table 30 config display set <index> rule <rule#>

LABEL	DESCRIPTION
`ACL rule number`	Shows the index number of this rule.
`ACL rule active`	Shows whether this rule is active or not.
`ACL rule action`	Shows the action taken when a packet matches a rule. The options are: `permit|drop|reject`.
`ACL rule protocol`	Shows the protocol number this rule applies to. They range from 0~255. For example, 1=ICMP, 6=TCP, 17=UDP, see RFC791.
`ACL rule log`	Shows whether the logging of packets matching the rule is enabled or not.
`ACL rule alert`	Shows whether or not an alert is sent when a packet matches the rule.
`Source Single IP address`	Shows the source IP address of packets to which the rule applies.

`Source IP address,`
`subnet mask`
	Shows the source IP address and subnet mask of packets to which the rule applies.

Table 30 config display set <index> rule <rule#>

LABEL	DESCRIPTION

`Source Starting IP address,`
`Ending IP address`
	Shows the range of source IP addresses of packets to which the rule applies.

`Destination Single IP address`	Shows the destination IP address of packets to which the rule applies.

`Destination IP address,`
`subnet mask`
	Shows the destination IP address and subnet mask of packets to which the rule applies.

`Destination Starting IP address,`
`Ending IP address`
	Shows the range of source IP addresses of packets to which the rule applies.

`TCP destination port number(s)`	Shows the destination TCP port of packets to which the rule applies.
`TCP destination port range(s)`	Shows the range of destination TCP port of packets to which the rule applies.
`UDP destination port number(s)`	Shows the destination UDP port of packets to which the rule applies.
`UDP destination port range(s)`	Shows the range of destination UDP ports of packets to which the rule applies.
`Custom dest. TCP/UDP port name`	Shows the name of the custom destination port.
`Custom IP protocol name`	Shows the name of a custom IP service.
`Custom ICMP protocol name`	Shows the name of a custom ICMP service.
`ACL rule name`	Shows the name of this rule.

The following table shows the interfaces assigned to each set number.

Table 31 Set-Interface Assignments

SET NUMBER	INTERFACE
1	LAN to WAN1
2	WAN1 to LAN
3	DMZ to LAN
4	DMZ to WAN1
5	WAN1 to DMZ
6	LAN to DMZ
7	LAN to LAN
8	WAN1 to WAN1
9	DMZ to DMZ
10	LAN to WLAN
11	WLAN to LAN
12	WAN1 to WLAN
13	WLAN to WAN1
14	DMZ to WLAN
15	WLAN to DMZ

Table 31 Set-Interface Assignments

SET NUMBER	INTERFACE
16	WLAN to WLAN
17	LAN to WAN2
18	WAN2 to LAN
19	WAN1 to WAN2
20	WAN2 to WAN
21	WAN2 to WAN2
22	DMZ to WAN2
23	WAN2 to DMZ
24	WLAN to WAN2
25	WAN2 to WLAN
26	LAN to VPN
27	VPN to LAN
28	WAN1 to VPN
29	VPN to WAN
30	WAN2 to VPN
31	VPN to WAN2
32	DMZ to VPN
33	VPN to DMZ
34	WLAN to VPN
35	VPN to WLAN
36	VPN to VPN

10.3.2 Anti-spam Example

This example shows how to set up an anti-spam blacklist filter, which is set to active, with an IP address of 192.168.1.33, and subnet mask of 255.255.255.255.

```
ras> config edit anti-spam rule 2 ip 2 active 1 address 192.168.1.33 netmask
255.255.255.255
ras> config save anti-spam
ras> config display anti-spam
ACL set header information:
ANTI_SPAM   ACL set number: 1
ANTI_SPAM   ACL set number of rules: 2
ANTI_SPAM   ACL set name: Anti-Spam
ACL set ANTI-SPAM Information:
ANTI_SPAM   ANTI_SPAM:DISABLE, WhiteList:DISABLE, BlackList:DISABLE
ANTI_SPAM   SPAM Mail Tag:[SPAM]
ANTI_SPAM   Phishing Mail Tag:[PHISHING]
ANTI_SPAM   Action:Add Tag to SMTP/POP3 SPAM Mail
ANTI_SPAM   Disable External Database
ANTI_SPAM   Action for Query timeout:Add Tag to SMTP/POP3 SPAM Mail
ACL rule header information:
ANTI_SPAM   ACL rule number: 1
ANTI_SPAM   ACL rule: White Rule
ACL rule header information:
ANTI_SPAM   ACL rule number: 2
ANTI_SPAM   ACL rule: Black Rule
ANTI_SPAM   Index:0, flags:1, IP:192.168.1.33 ,Netmask:255.255.255.255
```

The following table describes the fields displayed using the `config display set` command in the example above.

Table 32 config display set <entry#>

LABEL	DESCRIPTION
ANTI_SPAM ACL set number	Shows the index of this set.
ANTI_SPAM ACL set number of rules	Shows the number of rules in this set,
ANTI_SPAM ACL set name	Shows the name of the set.
ANTI_SPAM	Shows whether the anti-spam function is enabled or not.
WhiteList	Shows whether the whitelist service is enabled or not.
BlackList	Shows whether the blacklist function is enabled or not.
ANTI_SPAM SPAM Mail Tag	Shows the tag the antispam service attaches to mail identified as spam.
ANTI_SPAM Phishing Mail Tag	Shows the tag the antispam service attaches to mail identified as phishing mail.
ANTI_SPAM Action	Shows the action taken when the antispam service identifies mail as spam.
ANTI_SPAM Disable External Database	Shows whether an external database of known spam characteristics is used or not.
ANTI_SPAM Action for Query timeout	Shows the action taken when a query to an external database times out.

Table 32 config display set <entry#>

LABEL	DESCRIPTION
ANTI_SPAM ACL rule number	Shows the index number of a rule in the set. A set may only have two rules.
ANTI_SPAM ACL rule	Shows whether a rule in the set is based on a white or blacklist.
ANTI_SPAM Index XX, flags XX, IP: XXX.XXX.XXX.XXX, Netmask: XXX.XXX.XXX.XXX	Shows the email addresses, IP address/subnet masks, or MIME types/values that are included in the whitelist and blacklists of each rule. This example shows an IP address/ subnet mask based rule. The index shows the index number of an email address, IP address/subnet mask, or MIME type/value entry. A "0" flag indicates the rule is disabled, a non-zero flag shows it is enabled.

10.3.3 Custom Service Example

This example shows how to configure a custom service named "PERMITTED_ICMP", using ICMP protocol, of type 3 and code 1.

```
ras> config edit custom-service 1 name PERMITTED_ICMP
ras> config edit custom-service 1 ip-protocol icmp
ras> config edit custom-service 1 type 3
ras> config edit custom-service 1 code 1
ras> config save custom-service 1
ras> config display custom-service 1

 Custom Service #1:
   Custom Service Name: PERMITTED_ICMP
   Custom Service Type: ICMP
   Custom Service ICMP Type: 3
   Custom Service ICMP Code: 1
```

The following table describes the fields displayed using the `config display custom-service` command in the example above.

Table 33 config display custom-service

LABEL	DESCRIPTION
`Custom Service Name`	Shows the name for the service you have configured.
`Custom Service Type`	Shows the TCP/IP protocol selected for this service.
`Custom Service ICMP Type`	Shows the ICMP type. ICMP messages are assigned a type to indicate their use. For example, destination unreachable ICMP packets are identified by the value 3 in the type field.
`Custom Service ICMP Code`	Shows the ICMP code. The ICMP type can be further specified by the ICMP code. For example, type 3, code 3 ICMP packets indicate the host is unreachable.

11

Device Related Commands

Use these commands to configure dial-up WAN connections such as PPPoE (poe), PPTP (pne) and auxilary (aux) calls using the modem connected to the auxiliary port (if your ZyWALL has one).

11.1 Overview

A remote node is the remote gateway (and the network behind the remote gateway) across a WAN connection. Remote node 1 may be your ISP for example. You may configure multiple remote nodes in products with SMT menus or those with multiple WAN ports. In products without SMT menus or multiple WAN ports, a remote node is the ISP you configured in the web configurator.

A channel is a subset of an interface, such as a LAN or WAN interface. An interface may have more than one channel, but it usually has just one. The `channel-name` is the encapsulation method used for the WAN dial-up WAN link.

Table 34 Channel-name Command Input Values

LABEL	DESCRIPTION
channel-name	*poe0: poe0* is the PPPoE connection to WAN 1. *poe1: poe1* is the PPPoE connection to WAN 2 (if your ZyWALL has WAN 2). *pne0: pne0* is the PPTP connection to WAN 1. *pne1:pne1* is the PPTP connection to WAN 2 (if your ZyWALL has WAN 2). *aux0: aux0* is the connection using the modem connected to the auxiliary port (if your ZyWALL has one). *all: all* includes all the above mentioned channels.

11.2 Command Summary

The following section lists the commands for this feature.

Table 35 device Command Summary

COMMAND	DESCRIPTION	M
`device channel disp <CHANNEL_NAME> [LEVEL]`	Displays details on the specified channel, for example.	H+R+B
`device channel drop <`*`channel-name`*`>`	Drops the specified channel. *channel-name:* The options are `poe0|poe1|pne0|pne1|aux0|all`.	R+B
`device channel name <ALL|USE>`	Lists names of all channels or the names of the channels used.	H+R+B

Table 35 device Command Summary

COMMAND	DESCRIPTION	M
device channel threshold <channel_name> [NUMBER]	Sets the channel threshold.	H+R+B
device dial <*node#*>	Dials to a remote node. Enter sys rn disp to display a list of remote nodes to dial.	R

11.3 Command Example

This example triggers a call to the ISP.

```
ras> device dial 1
Start dialing for node <MyISP>...
```

12

Ethernet Commands

Use these commands to configure the settings of ethernet ports on ZyWALL.

12.1 Command Summary

The following section lists the commands for this feature.

Table 36 Ethernet Commands

COMMAND	DESCRIPTION	M
`ether edit load <ether-number>`	Loads the ethernet configuration for the specified interface. *ether-number*: Use the following for a ZyWALL with a single WAN Ethernet interface. 1: lan 2: wan 3: dmz 4: wlan Use the following for a ZyWALL with two WAN Ethernet interfaces. 1: lan 2: wan 3: dmz 4: wan2 5: wlan	R+B
`ether edit mtu <value>`	Sets the ethernet mtu size.	R+B
`ether edit speed <speed>`	Sets the ethernet speed in Mbps and duplex. *speed*: auto,10/full,10/half,100/full,100/half	R+B
`ether edit save`	Saves the ethernet configuration.	R+B
`ether dynamicPort set <port> <type>`	Sets the specified physical port mapping to DMZ, WLAN, or LAN. *port*: 1-4 *type*: DMZ, WLAN, LAN	R+B

12.2 Command Examples

This example changes the ZyWALL’s WAN speed to 10 Mbps and full duplex.

```
ras> ether edit load 2
ras> ether edit speed 10/full
ras> ether edit save
```

This example assigns the ZyWALL’s physical port 4 to be DMZ.

```
ras> ether dynamicPort set 4 DMZ
```

13

Firewall Commands

Use these commands to configure firewall settings on the ZyWALL.

13.1 Command Summary

The following table describes input values for some of the `firewall` commands. Other values are discussed with the corresponding commands.

Table 37 Firewall Command Input Values

LABEL	DESCRIPTION
from	A traffic source (where the traffic enters the ZyWALL). Use one of the following. `lan|wan1|wan2|dmz|wlan|vpn`
rule-number	The number of a specific firewall rule.
set-number	The number of a set of firewall rules. The firewall rules are grouped in sets by packet direction. Refer to Table 38 on page 87 for which set number to use for each firewall direction.
to	A traffic destination (where the traffic leaves the ZyWALL). Use one of the following. `lan|wan1|wan2|dmz|wlan|vpn`

Table 38 Firewall Set Numbers

FIREWALL DIRECTION	SET-NUMBER	FIREWALL DIRECTION	SET-NUMBER	FIREWALL DIRECTION	SET-NUMBER
LAN to WAN	1	WLAN to WAN	13	WAN2 to WLAN	25
WAN to LAN	2	DMZ to WLAN	14	LAN to VPN	26
DMZ to LAN	3	WLAN to DMZ	15	VPN to LAN	27
DMZ to WAN	4	WLAN to WLAN	16	WAN to VPN	28
WAN to DMZ	5	LAN to WAN2	17	VPN to WAN	29
LAN to DMZ	6	WAN2 to LAN	18	WAN2 to VPN	30
LAN to LAN	7	WAN to WAN2	19	VPN to WAN2	31
WAN to WAN	8	WAN2 to WAN	20	DMZ to VPN	32
DMZ to DMZ	9	WAN2 to WAN2	21	VPN to DMZ	33
LAN to WLAN	10	DMZ to WAN2	22	WLAN to VPN	34
WLAN to LAN	11	WAN2 to DMZ	23	VPN to WLAN	35
WAN to WLAN	12	WLAN to WAN2	24	VPN to VPN	36

The following section lists the `firewall` commands.

Table 39 Firewall Commands

COMMAND	DESCRIPTION	M
`sys firewall acl disp [`*`set-number`*`] [`*`rule-number`*`]`	Displays all of the firewall rules, rules for a specific direction of packet travel, or a a specific rule.	R+B
`sys firewall active <yes|no>`	Enables or disables the firewall.	R+B
`sys firewall cnt clear`	Clears the firewall log count.	R+B
`sys firewall cnt disp`	Displays the firewall log type and count.	R+B
`sys firewall dos display`	Displays the SMTP DoS defender setting.	R+B
`sys firewall dos ignore <lan|wan1|wan2|dmz|wlan|vpn> [on|off]`	Sets whether or not the firewall ignores DoS attacks on the specified interface.	R+B
`sys firewall dos smtp`	Enables or disables the SMTP Denial of Service (DoS) defender.	R+B
`sys firewall dynamicrule timeout [`*`value`*`]`	Sets the dynamic rule timeout value (in seconds). The value must be 8 or higher.	R+B
`sys firewall ignore logBroadcast <`*`from`*`> <`*`to`*`> <on|off>`	Sets whether or not the firewall ignores log broadcasts.	R+B
`sys firewall ignore triangle`	Sets if the firewall ignores triangle route packets on the LAN or WAN.	R+B
`sys firewall schedule display`	Displays the firewall schedule.	R+B
`sys firewall schedule load <`*`set-number rule-number`*`>`	Loads the firewall schedule by rule.	R+B
`sys firewall schedule save`	Saves and applies the firewall schedule.	R+B
`sys firewall schedule timeOfDay <always|`*`hh`*`:`*`mm hh`*`:`*`mm`*`>`	Sets what time the firewall schedule applies to.	R+B
`sys firewall schedule week allweek [on|off]`	Turns the firewall schedule on or off for all week.	R+B
`sys firewall schedule week friday [on|off]`	Turns the firewall schedule on or off for Fridays.	R+B
`sys firewall schedule week monday [on|off]`	Turns the firewall schedule on or off for Mondays.	R+B
`sys firewall schedule week saturday [on|off]`	Turns the firewall schedule on or off for Saturdays.	R+B
`sys firewall schedule week sunday [on|off]`	Turns the firewall schedule on or off for Sundays.	R+B
`sys firewall schedule week thursday [on|off]`	Turns the firewall schedule on or off for Thursdays.	R+B
`sys firewall schedule week tuesday [on|off]`	Turns the firewall schedule on or off for Tuesdays.	R+B
`sys firewall schedule week wednesday [on|off]`	Turns the firewall schedule on or off for Wednesdays.	R+B

13.2 Command Examples

This example displays the firewall log type and count.

```
ras> sys firewall cnt disp

ICMP Idle Timeout: 0               UDP Idle Timeout: 0
TCP Idle Timeout: 0                TCP SYN Idle Timeout: 0
TCP FIN Idle Timeout: 0
Land Attack: 0                     IP Spoof Attack: 0
ICMP Echo Attack: 0                ICMP Attack: 0
Netbios Attack: 0                  Trace Route Attack: 0
Tear Drop Attack: 0                Syn Flood Attack: 0
SMTP Attack: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
ACL name: ACL Default Set
  Blocks: 0                       Minute High: 0
  Max Incomplete High: 0          TCP Max Incomplete: 0
```

This example loads a firewall schedule for LAN to WAN firewall rule 1 and sets the schedule to apply the rule on all days of the week except Saturday and saves the schedule.

```
ras> sys firewall schedule load 2 1
Schedule Active(0=no, 1=yes): 0
ras> sys firewall schedule week monday off
Sun: 1, Mon: 0, Tue: 1, Wed: 1, Thu: 1, Fri: 1, Sat: 1.
Schedule Enable All Day On.
ras> sys firewall schedule save
Save schedule successful.
ras> sys firewall acl disp 2 1

ACL Runtime Data for ACL Set Number: 2
    Number of Rules: 2
        ACL default action (0=Drop, 1=Permit, 2=Reject): 0
    ICMP Idle Timeout: 0
    UDP Idle Timeout: 0
    TCP SYN Wait Timeout: 0
    TCP FIN Wait Timeout: 0
    TCP Idle Timeout: 0
    DNS Idle Timeout: 0
    Runtime Rule Number: 1
        Name: W2L_Rule_1        Active (0=no, 1=yes): 0
        Schedule (0=no, 1=yes): 1
        Sun: 1, Mon: 0, Tue: 1, Wed: 1, Thu: 1, Fri: 1, Sat: 1.
        Schedule Enable All Day On.
        Action (0=block, 1=permit, 2=reject): 1
        Log (0=disable, 1=enable, 2=not-m, 3=both): 0
        Alert (0=no, 1=yes): 0
        Protocol: 0
        Source IP Any: 1
        Source IP Number of Single: 0
        Source IP Number of Range: 0
        Source IP Number of Subnet: 0
        Dest IP Any: 1
        Dest IP Number of Single: 0
        Dest IP Number of Range: 0
        Dest IP Number of Subnet: 0
        TCP Source Port Any: 1
        TCP Source Port Number of Single: 0
        TCP Source Port Number of Range: 0
        UDP Source Port Any: 1
        UDP Source Port Number of Single: 0
        UDP Source Port Number of Range: 0
        TCP Dest Port Any: 0
        TCP Dest Port Number of Single: 0
        TCP Dest Port Number of Range: 0
        UDP Dest Port Any: 0
        UDP Dest Port Number of Single: 1
        UDP Dest Port Number of Range: 0
            Dest Port Single Port[1]: 68
        ICMP Custom Service Number with only Type defined: 0
        ICMP Custom Service Number with both Type and Code defined: 0
        Number of User Defined IP Protocol: 0
        ------------------------
```

14

IDP Commands

Use these commands to configure IDP (Intrusion Detection and Prevention) settings on the ZyWALL.

14.1 Command Summary

The following section lists the commands for this feature.

Table 40 IDP Commands

COMMAND	DESCRIPTION	M
`idp config clean`	Clears out all the IDP matrix settings.	R+B
`idp config dir dmz-dmz <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir dmz-lan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir dmz-wan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir dmz-wan2 <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir dmz-wlan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir lan-dmz <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir lan-lan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir lan-wan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir lan-wan2 <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir lan-wlan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wan2-lan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wan2-wan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wan2-wan2 <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wan2-wlan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wan-dmz <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wan-dmz <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wan-lan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wan-lan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wan-wan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wan-wan2 <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wan-wlan <on|off>`	Configures the protected traffic direction setting.	R+B

Table 40 IDP Commands (continued)

COMMAND	DESCRIPTION	M
`idp config dir wlan-dmz <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wlan-lan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wlan-wan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wlan-wan2 <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config dir wlan-wlan <on|off>`	Configures the protected traffic direction setting.	R+B
`idp config enable <on|off>`	Turns IDP on or off.	R+B
`idp config save`	Saves the enable setting and the protected traffic directions.	R+B
`idp config tune config l4cpmssck <on|off>`	Enables or disables the TCP packet header MSS check. This has the ZyWALL not check invalid packets, which can reduce the number of false alarms.	R+B
`idp config tune config l4Icmpcjsum <on|off>`	Enables or disables the ICMP packet header checksum check. This has the ZyWALL not check invalid packets, which can reduce the number of false alarms.	R+B
`idp config tune config l4Smtpasm <on|off>`	Enables or disables TCP assembly for SMTP. Disabling packet assembly can enhance throughput, but may allow more intrusions to go undetected.	R+B
`idp config tune config l4Tcpcksum <on|off>`	Enables or disables the TCP packet header checksum check. This has the ZyWALL not check invalid packets, which can reduce the number of false alarms.	R+B
`idp config tune config l4Tcpwindowck <on|off>`	Enables or disables the TCP packet window check. This has the ZyWALL not check invalid packets, which can reduce the number of false alarms.	R+B
`idp config tune config l4Udpcksum <on|off>`	Enables or disables the UDP packet header checksum check. This has the ZyWALL not check invalid packets, which can reduce the number of false alarms.	R+B
`idp config tune config l7Ftpasm <on|off>`	Enables or disables TCP assembly for FTP. Disabling packet assembly can enhance throughput, but may allow more intrusions to go undetected.	R+B
`idp config tune config l7Ftpdataasm <on|off>`	Enables or disables TCP assembly for FTPDATA. Disabling packet assembly can enhance throughput, but may allow more intrusions to go undetected.	R+B
`idp config tune config l7Httpasm <on|off>`	Enables or disables TCP assembly for HTTP. Disabling packet assembly can enhance throughput, but may allow more intrusions to go undetected.	R+B
`idp config tune config l7Otherasm <on|off>`	Enables or disables TCP assembly for other protocols. Disabling packet assembly can enhance throughput, but may allow more intrusions to go undetected.	R+B
`idp config tune config l7Pop3asm <on|off>`	Enables or disables TCP assembly for POP3. Disabling packet assembly can enhance throughput, but may allow more intrusions to go undetected.	R+B
`idp config tune display`	Displays the tune configuration.	R+B
`idp config tune load`	Loads the tune configuration. IDP tuning allows you to enable or disable packet header checks and packet assembly.	R+B
`idp config tune save`	Saves the tune configuration.	R+B
`idp display`	Displays whether or not IDP is enabled and what traffic flows the ZyWALL checks for intrusions.	R+B

Table 40 IDP Commands (continued)

COMMAND	DESCRIPTION	M
`idp load`	Loads the enable setting and the protected traffic directions.	R+B
`idp signature config action <1~6>`	Sets the action the ZyWALL takes upon finding a match for the signature. 1: No Action. The intrusion is detected but no action is taken. 2: Drop Packet. The packet is silently discarded. 3: Drop Session. When the firewall is enabled, subsequent TCP/IP packets belonging to the same connection are dropped. Neither sender nor receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. 4: Reset Sender. When the firewall is enabled, the TCP/IP connection is silently torn down. Just the sender is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. 5: Reset Receiver When the firewall is enabled, the TCP/IP connection is silently torn down. Just the receiver is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. 6: Reset Both. When the firewall is enabled, the TCP/IP connection is silently torn down. Both sender and receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.	R+B
`idp signature config active <on|off>`	Enables or disables the signature.	R+B
`idp signature config alert <on|off>`	Enables or disables the sending of an alert e-mail when a match is found for the signature.	R+B
`idp signature config log <on|off>`	Enables or disables log generation when a match is found for the signature.	R+B
`idp signature display`	Displays the currently loaded signature's settings.	R+B
`idp signature load <`*`signature-id`*`>`	Loads the specified signature (so you can configure it). *`signature-id`*: Each intrusion signature has a unique identification number. This number may be searched at myZyXEL.com for more detailed information.	R+B
`idp signature reset`	Resets the signature setting to its default settings.	R+B
`idp signature save`	Saves the signatures settings.	R+B
`idp update config autoupdate <on|off>`	Enables or disables automatic updating of IDP signatures.	R+B
`idp update config dailyTime <00~23>`	Sets the hour for daily updates.	R+B
`idp update config method <1~3>`	Sets how often to update the IDP signatures. 1: hourly 2: daily 3:weekly	R+B
`idp update config weeklyDay <1~7>`	Sets the day for weekly updates.	R+B
`idp update config weeklyTime <00~23>`	Sets the hour for weekly updates.	R+B
`idp update display`	Shows signature information and the update setting.	R+B
`idp update load`	Loads the signature update settings.	R+B

Table 40 IDP Commands (continued)

COMMAND	DESCRIPTION	M
`idp update save`	Saves the signature update settings.	R+B
`idp update start`	Starts the signature update.	R+B

14.2 Command Examples

This example loads signature 1051222 and displays its current settings. Then it sets the ZyWALL to send an alert upon finding a match for the signature. Finally it saves the signature's settings.

```
ras> idp signature load 1051222
ras> idp signature display
 RuleID : 1051222 AttackType : SPAM
 Platform : Windows,UNIX,NetworkDevice Severity : Medium
 Name : SPAM Drug
 Active : On
 Log : On
 Alert : Off
 Action : Drop Session
ras> idp signature config alert on
ras> idp signature display
 RuleID : 1051222 AttackType : SPAM
 Platform : Windows,UNIX,NetworkDevice Severity : Medium
 Name : SPAM Drug
 Active : On
 Log : On
 Alert : On
 Action : Drop Session
ras> idp signature save
```

15

IP Commands

Use these commands to configure IP settings on the ZyWALL.

15.1 Command Summary

The following table describes input values for some of the `ip` commands. Other values are discussed with the corresponding commands.

Table 41 IP Command Input Values

LABEL	DESCRIPTION
isp-group-idx	The number of an ISP configuration on the ZyWALL. For example, the ISP configured for the WAN 1 interface is ISP group index 1.0
number	The number of system report records to display. For example, if you specify 10, the top 10 report entries display.

15.1.1 ALG Commands

The following section lists the ALG commands.

Table 42 ALG Commands

COMMAND	DESCRIPTION	M
`ip alg disable <ALG_FTP|ALG_H323|ALG_SIP>`	Turns off the specified ALG (Application Layer Gateway).	R+B
`ip alg disp`	Shows whether the ALG is enabled or disabled.	R+B
`ip alg enable <ALG_FTP|ALG_H323|ALG_SIP>`	Turns on the specified ALG.	R+B
`ip alg ftpPortNum [`*port*`]`	Sets the FTP ALG to support a different port number (instead of the default).	R+B
`ip alg siptimeout <`*timeout*`>`	Sets the SIP timeout in seconds. 0 means no timeout.	R+B

15.1.2 ARP Commands

The following section lists the ARP commands.

Table 43 ARP Commands

COMMAND	DESCRIPTION	M
`ip arp ackGratuitous active [yes|no]`	Turns the acceptance of gratuitous ARP (Address Resolution Protocol) packets on or off. See Section 15.1.3 on page 98 for details.	R+B
`ip arp ackGratuitous forceUpdate [on|off]`	Has the ZyWALL update an existing ARP entry for which a gratuitous request was received. See Section 15.1.3 on page 98 for details.	R+B
`ip arp add <ip-address> ether <mac-address>`	Adds ARP information.	R+B
`ip arp attpret <on|off>`	Allows or disallows ZyWALL to receive ARP from a different network or not.	R+B
`ip arp force <on|off>`	Enables or disables the ARP timeout function.	R+B
`ip arp gratuitous <on|off>`	Turns duplicate IP address detection (based on gratuitous ARPs) on or off.	R+B
`ip arp status <interface>`	Displays an interface’s ARP status.	R+B
`ip arp reqUpdateTable <on|off>`	Sets whether or not the ZyWALL updates its ARP table based on the source IP address and MAC address of received ARP request packets. This is off by default. If you turn this on, the setting changes back to off when the ZyWALL restarts.	R+B

15.1.3 ARP Behavior and the ARP ackGratuitous Command Details

The ZyWALL does not accept ARP reply information if the ZyWALL did not send out a corresponding request. This helps prevent the ZyWALL from updating its ARP table with an incorrect IP address to MAC address mapping due to a spoofed ARP. An incorrect IP to MAC address mapping in the ZyWALL’s ARP table could cause the ZyWALL to send packets to the wrong device.

15.1.3.1 Commands for Using or Ignoring Gratuitous ARP Requests

A gratuitous ARP request is an ARP request that a host sends to resolve its own IP address. The packet uses the host’s own IP address as the source and destination IP address. The packet uses the Ethernet broadcast address (FF:FF:FF:FF:FF:FF) as the destination MAC address. This is used to determine if any other hosts on the network are using the same IP address as the sending host. The other hosts in the network can also update their ARP table IP address to MAC address mappings with this host’s MAC address.

The `ip arp ackGratuitous` commands set how the ZyWALL handles gratuitous ARP requests.

- Use `ip arp ackGratuitous active no` to have the ZyWALL ignore gratuitous ARP requests.
- Use `ip arp ackGratuitous active yes` to have the ZyWALL respond to gratuitous ARP requests.

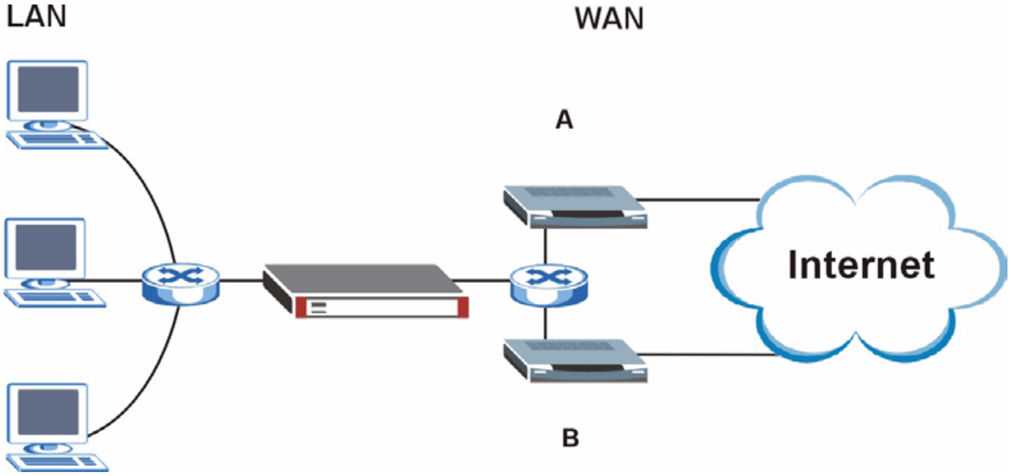
For example, say the regular gateway goes down and a backup gateway sends a gratuitous ARP request. If the request is for an IP address that is not already in the ZyWALL's ARP table, the ZyWALL sends an ARP request to ask which host is using the IP address. After the ZyWALL receives a reply from the backup gateway, it adds an ARP table entry.

If the ZyWALL's ARP table already has an entry for the IP address, the ZyWALL's response depends on how you configure the `ip arp ackGratuitous forceUpdate` command.

- Use `ip arp ackGratuitous forceUpdate on` to have the ZyWALL update the MAC address in the ARP entry.
- Use `ip arp ackGratuitous forceUpdate off` to have the ZyWALL not update the MAC address in the ARP entry.

A backup gateway (as in the following graphic) is an example of when you might want to turn on the forced update for gratuitous ARP requests. One day gateway A shuts down and the backup gateway (B) comes online using the same static IP address as gateway A. Gateway B broadcasts a gratuitous ARP request to ask which host is using its IP address. If ackGratuitous is on and set to force updates, the ZyWALL receives the gratuitous ARP request and updates its ARP table. This way the ZyWALL has a correct gateway ARP entry to forward packets through the backup gateway. If ackGratuitous is off or not set to force updates, the ZyWALL will not update the gateway ARP entry and cannot forward packets through gateway B.

Figure 3 Backup Gateway



Updating the ARP entries could increase the danger of spoofing attacks. It is only recommended that you turn on ackGratuitous and force update if you need it like in the previous backup gateway example. Turning on the force updates option is more dangerous than leaving it off because the ZyWALL updates the ARP table even when there is an existing entry.

15.1.4 Binding Commands

The following section lists the commands for having a (non-WAN) Ethernet interface filter packets based on IP address to MAC address binding.

Table 44 Binding Commands

COMMAND	DESCRIPTION	M
ip binding <enif*x*> active <yes|no>	Enable this to have the specified interface accept traffic only from devices which have received an IP address from the ZyWALL.	R+B
ip binding <enif*x*> exempt active <yes|no>	Sets whether or not the ZyWALL packets from a range of source IP addresses that were not assigned by the ZyWALL.	R+B
ip binding <enif*x*> exempt range <*start-ip*> <*end-ip*>	Sets the range of IP addresses that are exempt from IP to MAC address binding on the specified interface.	R+B
ip binding <enif*x*> status	Displays the IP/MAC binding settings for the specified interface.	R+B

15.1.5 Content Filtering Commands

The following section lists the content filtering commands.

Table 45 Content Filtering Commands

COMMAND	DESCRIPTION	M
ip cf bypass [LAN|DMZ|WAN] [on|off]	Sets content filtering to ignore an interface’s web traffic.	R+B
ip cf common denymsg [*message*]	Sets or displays the content filtering denied access message.	R+B
ip cf common display	Shows the general content filtering settings.	R+B
ip cf common enable <on|off>	Turns content filtering on or off.	R+B
ip cf common redirurl [*url*]	Sets or displays the content filtering denied access redirect URL.	R+B
ip cf externalDB cache delete <*entry_number*|All>	Removes an individual entry from the cache of URLs rated by the external content filter server or clears the entire cache.	R+B
ip cf externalDB cache display	Displays the category ratings of URLs that the ZyWALL has received from the external content filter server.	R+B
ip cf externalDB cache timeout [*hours*]	Sets how many hours a categorized web site address remains in the cache.	R+B
ip cf externalDB enable [on|off]	Turns the external database checking on or off.	R+B
ip cf externalDB enableLog <on|off>	Turns content filtering external database logs on or off.	R+B
ip cf externalDB exDblogserver [*server-address*]	Sets the address for content filtering external database logs.	R+B
ip cf externalDB matchweb [none log|block|both]	Sets the log and block action for websites that match a category in the content filtering external database configuration.	R+B

Table 45 Content Filtering Commands (continued)

COMMAND	DESCRIPTION	M
`ip cf externalDB queryURL <index> <url> <Server|localCache>`	Checks whether or not the content filter policy currently blocks any given web page. `Server`: Test whether or not the web site above is saved in the external content filter server's database of restricted web pages. `localCache`: test whether or not the web site above is saved in the ZyWALL's database of restricted web pages.	R+B
`ip cf externalDB reginfo display`	Displays the content filtering external database registration information.	R+B
`ip cf externalDB reginfo refresh`	Refreshes and displays the content filtering external database registration license.	R+B
`ip cf externalDB serverList display`	Displays the list of external database content filtering servers.	R+B
`ip cf externalDB serverList refresh`	Updates and displays the list of external database content filtering servers.	R+B
`ip cf externalDB serverunavailable [none|log|block|both]`	Sets the log and block action for when there is no response from the content filtering external database configuration.	R+B
`ip cf externalDB unratedweb [none|log|block|both]`	Sets the log and block action for websites that are note rated by the content filtering external database configuration.	R+B
`ip cf externalDB waitingTime [seconds]`	Specifies a number of seconds (1~30) for the ZyWALL to wait for a response from the external content filtering server. The server is considered unavailable it there is still no response by the time this period expires.	R+B
`ip cf object add <trust|untrust|keyword> <string>`	Creates a content filtering object.	R+B
`ip cf object delete <trust|untrust|keyword> <index>`	Removes the specified content filtering object. Subsequent objects move up one.	R+B
`ip cf object display`	Displays the content filtering objects.	R+B
`ip cf object save`	Saves the content filtering object configuration.	R+B
`ip cf policy config customRule add [trust|untrust|keyword] [index]`	Adds a customized content filter policy to the policy. First use the `ip cf object` commands to create the global list of trusted and untrusted websites and keywords that you can use in individual policies. Entering the command without any parameters displays the global list of objects.	R+B
`ip cf policy config customRule delete [index]`	Removes the specified customized content filter policy from the policy. Enter the command without specifying a customized content filter policy to see the customized content filter policy numbers.	R+B
`ip cf policy config customRule display`	Displays the policy's customized content filter policies.	R+B
`ip cf policy config customRule enable <on|off>`	Turns the policy's customized content filter policies on or off.	R+B

Table 45 Content Filtering Commands (continued)

COMMAND	DESCRIPTION	M
`ip cf policy config CustomizedFlags [filterList|customize|disableAllExceptTrusted|unblockRWFToTrusted|keywordBlock|fullPath|caseInsensitive|fileName] [enable|disable]`	Turns the content filtering policy on or off and sets its customized settings. `filterList`: Use this to enable or disable the content filtering policy. `customize`: Sets whether or not to filter web access based on the policy's list of trusted and forbidden web sites and forbidden key words. Content filter list customization may be enabled and disabled without re-entering these site names. `disableAllExceptTrusted`: Block all web access except the listed trusted web sites,. `unblockRWFToTrusted`: Allows access to restricted web features only on trusted web sites. `kewordBlock`: Block access to websites with URLs that contain specified keywords in the domain name or IP address. `fullPath`: Full path has the ZyWALL check all characters that come before the last slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/. `caseInsensitive`: Sets whether or not the content filtering policy's customized settings are case-sensitive. `fileName`: Filename URL checking has the ZyWALL check all of the characters in the URL. For example, filename URL checking searches for keywords within the URL www.zyxel.com.tw/news/pressroom.php. `[enable|disable]`: Turn the content filtering policy or its customized settings on or off.	R+B
`ip cf policy config enable <on|off>`	Turns the content filtering policy on or off.	R+B
`ip cf policy config ipGroup add <1:Single|2:Subnet|3:Range> <`*`ip-address1`*`> [`*`mask`*`|`*`ip-address2`*`]`	Adds an IP group to the policy.	R+B
`ip cf policy config ipGroup delete <`*`index`*`>`	Removes an IP group from the policy.	R+B
`ip cf policy config ipGroup display`	Displays the content filtering policy's IP groups.	R+B
`ip cf policy config name <`*`name`*`>`	Sets the content filtering policy's name. You must use `ip cf policy insert` or `ip cf policy edit` command before you can use the `config` commands.	R+B
`ip cf policy config schedule display`	Displays the content filtering policy's schedule configuration.	R+B
`ip cf policy config schedule eachDay timeSeg1 <1~7:weekday> <0~24:start hour> <0~59:start minute> <0~24:end hour> <0~59:end minute>`	Sets the content filtering policy's individual day schedule's first time segment.	R+B
`ip cf policy config schedule eachDay timeSeg2 <1~7:weekday> <0~24:start hour> <0~59:start minute> <0~24:end hour> <0~59:end minute>`	Sets the content filtering policy's individual day schedule's second time segment.	R+B

Table 45 Content Filtering Commands (continued)

COMMAND	DESCRIPTION	M
`ip cf policy config schedule enable <on|off>`	Turns the content filtering policy's schedule on or off.	R+B
`ip cf policy config schedule everyday timeSeg1 <0~24:start hour> <0~59:start minute> <0~24:end hour> <0~59:end minute>`	Sets the content filtering policy's everyday schedule's first time segment.	R+B
`ip cf policy config schedule everyday timeSeg2 <0~24:start hour> <0~59:start minute> <0~24:end hour> <0~59:end minute>`	Sets the content filtering policy's everyday schedule's second time segment.	R+B
`ip cf policy config schedule type[1:always|2:everyday|3:policies for each day]`	Sets the content filtering policy's schedule to apply everyday or only during specific time interval(s) of specific day(s).	R+B
`ip cf policy config webControl category <block|forward> <1~61|All>`	Sets which content filtering categories the policy allows or blocks based on the external database service's rating. Use `ip cf policy config webControl display` to see the available categories.	R+B
`ip cf policy config webControl display`	Displays the policy's current external database categories.	R+B
`ip cf policy config webControl enable <on|off>`	Turns the external database service content filtering (category-based content filtering) on or off.	R+B
`ip cf policy config webFeature [<block|nonblock> <activex|java|cookie|webproxy>]`	Sets the content filtering policy to block (or not block) ActiveX controls, Java applets, cookies and disable web proxies.	R+B
`ip cf policy delete <`*`index`*`>`	Removes the specified content filtering policy.	R+B
`ip cf policy display <`*`index`*`>`	Displays information about the specified content filtering policy.	R+B
`ip cf policy displayAll`	Lists the content filtering policies.	R+B
`ip cf policy edit <`*`index`*`>`	Lets you edit the specified content filtering policy.	R+B
`ip cf policy insert <`*`index`*`>`	Adds a content filtering policy at the specified number. You must use this or the `edit` command before you can use the `ip cf policy config` commands.	R+B
`ip cf policy save`	Saves and applies the content filtering policy.	R+B

15.1.6 Content Filtering Command Examples

The following commands configure example content filtering trusted and untrusted web site objects and keyword objects.

```
ras> ip cf object add trust www.good.com
ras> ip cf object add trust www.my-company-example.com
ras> ip cf object add untrust www.bad.com
ras> ip cf object add untrust www.hacking-example.com
ras> ip cf object add keyword porn
ras> ip cf object add keyword hacking
ras> ip cf object display
Object list:

    Trusted domain
    ----------------------------------------
    [1] www.good.com
    [2] www.my-company-example.com

    Untrusted domain
    ----------------------------------------
    [1] www.bad.com
    [2] www.hacking-example.com

    Keyword
    ----------------------------------------
    [1] porn
    [2] hacking
ras> ip cf object save
```

The following example enables content filtering, loads content filtering policy one, configures it with the following settings, and saves it.

- Content Filtering: Enabled
- Policy: Enabled
- IP Group: IP addresses 192.168.1.33-192.168.1.66
- Customized Rule Enforcement: Enabled
- Customized Rule: Untrusted, www.hacking-example.com
- Web Feature Blocking: Block java
- Schedule: Enabled
- Schedule Type: Everyday

- Schedule Period: 9:00 A.M. to 5:30 P.M.

```
ras> ip cf common enable on
ras> ip cf policy insert 1
ras> ip cf policy config enable on
ras> ip cf policy config ipGroup add 3 192.168.1.33 192.168.1.66
ras> ip cf policy config customRule enable on
ras> ip cf object display
Object list:

    Trusted domain
    ----------------------------------------
    [1] www.good.com
    [2] www.my-company-example.com

    Untrusted domain
    ----------------------------------------
    [1] www.bad.com
    [2] www.hacking-example.com

    Keyword
    ----------------------------------------
    [1] porn
    [2] hacking
ras> ip cf policy config customRule add untrust 2
ras> ip cf policy config webFeature block java
Usage:[block/nonblock] [activex/java/cookie/webproxy]
Resrict Web Feature:
    ActiveX: Forward
    Java   : Block
    Cookie : Forward
    Proxy  : Forward
ras> ip cf policy config schedule enable on
ras> ip cf policy config schedule type 2
ras> ip cf policy config schedule everyday timeSeg1 9 00 17 30
ras> ip cf policy save
```

The following example changes the schedule to policies for each day and applies it only on Mondays.

```
ras> ip cf policy edit 1
ras> ip cf policy config schedule type 3
ras> ip cf policy config schedule eachDay timeSeg1 2 9 00 17 30
```

The following command removes the policy's customized rule entry for www.hacking-example.com.

```
as> ip cf policy config customRule delete
Usage:[index]
========================
[Index: 1] [Type: Not Trust Domain] Name: www-hacking-example.com
ras> ip cf policy config customRule delete 1
```

15.1.7 Custom Port Commands

The following section lists the custom port commands.

Table 46 Custom Port Commands

COMMAND	DESCRIPTION	M
ip customizePort config <*index*> name <FTP|H323|SIP> <*start-port*> <*end-port*>	Modifies or adds a new customized port rule for FTP, H.323, or SIP traffic. *index*: The number of a customized port rule (1~12).	R+B
ip customizePort delete <*index*>	Deletes the specified customized port rule.	R+B
ip customizePort display	Displays all customized port rules.	R+B

15.1.8 DHCP Commands

The following section lists the DHCP commands.

Table 47 DHCP Commands

COMMAND	DESCRIPTION	M
ip dhcp <*interface*> client release	Releases the specified interface's DHCP client IP address. The interface must be a DHCP client to use this command.	R
ip dhcp <*interface*> client renew	Renews the DHCP client IP address. The interface must be a DHCP client to use this command.	R
ip dhcp <*interface*> status	Displays the DHCP status of the specified interface.	R

15.1.9 DNS Commands

The following section lists DNS commands.

Table 48 DNS Commands

COMMAND	DESCRIPTION	M
ip dns dmz display	Shows the DNS server settings the ZyWALL assigns to DMZ DHCP clients.	R
ip dns dmz edit <0|1|2> <0:from ISP|1:user defined|2:DNS relay|3:none> [*isp-idx*|*ip-address*]	Configures the DNS server settings the ZyWALL assigns to DMZ DHCP clients. 0|1|2: Specifies the first, second, or third DNS server setting. *isp-idx*|*ip-address*: If you set the server as from ISP (0), specify the number of the ISP (the number of the remote node). If you set the server as user defined (1), specify the IP address.	R
ip dns lan display	Shows the LAN DHCP DNS server settings.	R

Table 48 DNS Commands (continued)

COMMAND	DESCRIPTION	M
`ip dns lan edit <0|1|2> <0:from ISP|1:user defined|2:DNS relay|3:none> [`*`isp-idx`*`|`*`ip-address`*`]`	Configures the DNS server settings the ZyWALL assigns to LAN DHCP clients. `0|1|2`: Configures the first, second, or third DNS server setting. `0:from ISP|1:user defined|2:DNS relay|3:none`: If you set the server as from ISP (0), specify the number of the ISP. If you set the server as user defined (1), specify the IP address. *`isp-idx`*`|`*`ip-address`*: The number of the ISP (the number of the remote node) or the IP address of the DNS server.	R
`ip dns lan edit <0|1|2> <0:from ISP|1:user defined|2:DNS relay|3:none> [`*`isp-idx`*`|`*`ip-address`*`]`	Configures the DNS server settings the ZyWALL assigns to LAN DHCP clients. `0|1|2`: Configures the first, second, or third DNS server setting. `0:from ISP|1:user defined|2:DNS relay|3:none`: If you set the server as from ISP (0), specify the number of the ISP. If you set the server as user defined (1), specify the IP address. *`isp-idx`*`|`*`ip-address`*: The number of the ISP (the number of the remote node) or the IP address of the DNS server.	R
`ip dns query address <`*`ip-address`*`> [`*`timeout`*`]`	Displays the domain name of an IP address. *`timeout`*`:` The maximum number of seconds to wait for a response.	R
`ip dns query name <`*`domain-name`*`>`	Displays the IP address of a domain name.	R
`ip dns system cache disp <0~5> [0:increase|1:decrease]`	Displays the DNS cache table. Select which criteria to sort the entries by. `0`: Displays the entries by the time they were created. `1`: Sorts the entries by domain name or URL. `2`: Sorts the entries by type (positive or negative). `3`: Sorts the entries by IP address. `4`: Sorts the entries by the number of times the entry was used. `5`: Sorts the entries by Time To Live (number of seconds left before the DNS resolution entry is discarded from the cache). `0:increase|1:decrease`: Specify ascending or descending order.	R+B
`ip dns system cache flush`	Clears the DNS cache.	R+B
`ip dns system cache negaperiod <60~3600>`	Sets the number of seconds negative DNS entries stay in the cache.	R+B
`ip dns system cache negative <0:disable|1:enable>`	Enables or disables the DNS negative cache.	R+B
`ip dns system cache positive <0:disable|1:enable>`	Enables or disables the DNS positive cache.	R+B
`ip dns system cache ttl <60~3600>`	Sets the positive DNS cache maximum TTL (Time To Live).	R+B
`ip dns system dela <`*`index`*`>`	Removes the specified DNS address record entry.	R+B
`ip dns system delns <`*`index`*`>`	Removes the specified DNS name server record entry.	R+B
`ip dns system display`	Shows the system DNS server settings.	R+B

Table 48 DNS Commands (continued)

COMMAND	DESCRIPTION	M
`ip dns system edita <index> <name> <0:FQDN|1:wildcard> <0:from ISP group|1:user defined> <isp-group-idx|ip-address>`	Edits the specified DNS address record.	R+B
`ip dns system editns <index> <*|domain name> <0:from ISP|1:user defined (public)|2: user defined (private)> <isp-group-idx|dns-server-ip>`	Edits the specified DNS name server record.	R+B
`ip dns system inserta <before record idx|-1:new> <name> <0:FQDN|1:wildcard> <0:from ISP group|1:user defined> <isp-group-idx|ip-address>`	Inserts a DNS address record.	R+B
`ip dns system insertns <before record idx|-1:new> <*|domain name> <0:from ISP|1:user defined (public)|2: user defined (private)> <isp-group-idx|dns-server-ip>`	Inserts a DNS name server record.	R+B
`ip dns system movea <index <index>`	Moves the specified DNS address record entry to the specified entry number.	R+B
`ip dns system movens <index> <index>`	Moves the specified DNS name server record entry to the specified entry number.	R+B
`ip dns wlan display`	Shows the WLAN DHCP DNS server settings.	R
`ip dns wlan edit <0|1|2> <0:from ISP|1:user defined|2:DNS relay|3:none> [isp-idx|ip-address]`	Configures the DNS server settings the ZyWALL assigns to wlan DHCP clients. `0|1|2`: Configures the first, second, or third DNS server setting. `0:from ISP|1:user defined|2:DNS relay|3:none`: If you set the server as from ISP (0), specify the number of the ISP. If you set the server as user defined (1), specify the IP address. *`isp-idx|ip-address`*: The number of the ISP (the number of the remote node) or the IP address of the DNS server.	R

15.1.10 DNS Command Examples

The following example configures the DNS server settings the ZyWALL assigns to LAN DHCP clients. In this case the first DNS server is the one assigned by ISP 1. The second DNS server is at IP address 192.168.1.5. No third DNS server is assigned.

```
ras> ip dns lan edit 0 0 1 1
ras> ip dns lan edit 1 1 192.168.1.5
ras> ip dns lan edit 2 3
ras> ip dns lan display
Router assigned DNS servers to host
===================================
First DNS server is from WAN_1, DNS server index 1
Second DNS server is user defined: 192.168.1.5
Third DNS server is none
```

This example does the following.

1. Inserts a new DNS address record named example for www.my-company.com.example for the WAN 1 interface.
2. Inserts a new DNS address record named example for a private DNS server for www.my-company-1.com.example.
3. Displays the system DNS server settings.

```
ras> ip dns system inserta -1 www.my-company.com.example 0 0 1
ras> ip dns system insertns -1 www.mycompany-2.com.example 2 10.0.0.5
ras> ip dns system display
System DNS HA and Proxy Service Configuration
=============================================

Rule Summary: A Record
001 | record type=A Record, ISP=WAN_1
    | FQDN       =www.my-company.com.example

Rule Summary: NS Record
001 | record type=NS Record, DNS server=10.0.0.5(private)
    | Domain Name=www.mycompany-2.com.example
```

15.1.11 HTTP Commands

The following section lists the HTTP commands.

Table 49 HTTP Commands

COMMAND	DESCRIPTION	M
`ip httpClient debug <on|off>`	Turns the HTTP client debug messages on or off.	R+B
`ip httpClient display`	Displays the system HTTP client state.	R+B
`ip httpd debug [on|off]`	Displays or sets the web configurator debug flag.	R+B

15.1.12 ICMP Commands

The following section lists the ICMP commands.

Table 50 ICMP Commands

COMMAND	DESCRIPTION	M
`ip icmp discovery <interface> [on|off]`	Turns ICMP discovery (ICMP type 10, RFC 1256) off or on for the specified interface (or IP alias on an interface).	R+B
`ip icmp sourcequench [on|off]`	Displays or sets the ignore ICMP source quench packets flag. Enable the ignore ICMP source quench packets flag to have the ZyWALL not log ICMP source quench packets.	R
`ip icmp status`	Displays the ICMP statistics counter.	R+B

15.1.13 ICMP Command Example

The following example displays the ICMP status.

```
ras> ip icmp status
( 1)icmpInMsgs                   0     (14)icmpOutMsgs              1628
( 2)icmpInErrors                 0     (15)icmpOutErrors               0
( 3)icmpInDestUnreachs           0     (16)icmpOutDestUnreachs         0
( 4)icmpInTimeExcds              0     (17)icmpOutTimeExcds            0
( 5)icmpInParmProbs              0     (18)icmpOutParmProbs            0
( 6)icmpInSrcQuenchs             0     (19)icmpOutSrcQuenchs           0
( 7)icmpInRedirects              0     (20)icmpOutRedirects            0
( 8)icmpInEchos                  0     (21)icmpOutEchos             1614
( 9)icmpInEchoReps               0     (22)icmpOutEchoReps             0
(10)icmpInTimestamps             0     (23)icmpOutTimestamps           0
(11)icmpInTimestampReps          0     (24)icmpOutTimestampReps        0
(12)icmpInAddrMasks              0     (25)icmpOutAddrMasks            0
(13)icmpInAddrMaskReps           0     (26)icmpOutAddrMaskReps         0
```

The following table describes the labels in this display.

Table 51 ip icmp status Description

LABEL	DESCRIPTION
icmpInMsgs	The number of ICMP messages received on the interface.
icmpInErrors	The number of ICMP messages with an error received on the interface.
icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received on the interface.
icmpInTimeExcds	The number of ICMP Time Exceeded messages received on the interface.
icmpInParmProbs	The number of ICMP Parameter Problem messages received on the interface.
icmpInSrcQuenchs	The number of ICMP Source Quench messages received on the interface.
icmpInRedirects	The number of ICMP Redirect messages received on the interface.
icmpInEchos	The number of ICMP Echo (request) messages received on the interface.
icmpInEchoReps	The number of ICMP Echo Reply messages received on the interface.
icmpInTimestamps	The number of ICMP Timestamp messages received on the interface.

Table 51 ip icmp status Description

LABEL	DESCRIPTION
icmpInTimestampReps	The number of ICMP Timestamp Reply messages received on the interface.
icmpInAddrMasks	The number of ICMP Address Mask Request messages received on the interface.
icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received on the interface.
icmpOutMsgs	The number of ICMP messages received sent through the interface.
icmpOutErrors	The number of ICMP messages with an error sent through the interface.
icmpOutDestUnreach	The number of ICMP Destination Unreachable messages sent through the interface.
icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent through the interface.
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent through the interface.
icmpOutSrcQuench	The number of ICMP Source Quench messages sent through the interface.
icmpOutRedirects	The number of ICMP Redirect messages sent through the interface.
icmpOutEchos	The number of ICMP Echo (request) messages sent through the interface.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent through the interface.
icmpOutTimestamps	The number of ICMP Timestamp messages sent through the interface.
icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent through the interface.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent through the interface.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent through the interface.

15.1.14 IGMP Commands

The following section lists the IGMP commands.

Table 52 IGMP Commands

COMMAND	DESCRIPTION	M
`ip igmp debug [0:off|1:normal|2:detailed]`	Sets the IGMP debug level.	R
`ip igmp forwardall [on|off]`	Activates or deactivates IGMP forwarding to all interfaces.	R
`ip igmp iface <`*`interface`*`> grouptm <260~2147483647>`	Sets the IGMP group timeout (in seconds) for the specified interface (or IP alias on an interface).	R
`ip igmp iface <`*`interface`*`> interval <125~2147483647>`	Sets the IGMP query interval (in seconds) for the specified interface (or IP alias on an interface).	R
`ip igmp iface <`*`interface`*`> join <`*`group`*`>`	Adds the specified interface (or IP alias on an interface) to the specified IGMP group.	R
`ip igmp iface <`*`interface`*`> leave <`*`group`*`>`	Removes the specified interface (or IP alias on an interface) from the specified IGMP group.	R

Table 52 IGMP Commands (continued)

COMMAND	DESCRIPTION	M
`ip igmp iface <`*`interface`*`> query`	Sends an IGMP query on the specified interface (or IP alias on an interface).	R
`ip igmp iface <`*`interface`*`> rsptime [100~255]`	Sets the IGMP response time in tenths (1/10) of a second for the specified interface (or IP alias on an interface).	R
`ip igmp iface <`*`interface`*`> start`	Turns on IGMP on the specified interface (or IP alias on an interface).	R
`ip igmp iface <`*`interface`*`> stop`	Turns off IGMP on the specified interface (or IP alias on an interface).	R
`ip igmp iface <`*`interface`*`> ttl <0~2147483647>`	Sets the IGMP Time To Live threshold for the specified interface (or IP alias on an interface).	R
`ip igmp iface <`*`interface`*`> v1compat [on|off]`	Turns IGMP version 1 compatibility on or off for the specified interface (or IP alias on an interface).	R
`ip igmp querier [on|off]`	Turns the IGMP stop query flag on or off.	R
`ip igmp robustness [2~2147483647|no]`	Sets the number of times that the ZyWALL sends IGMP group-specific queries before declaring a group to no longer have any members on an interface. (RFC 2236) no: restores the default value, 2.	R
`ip igmp status`	Displays the IGMP status.	R

15.1.15 IGMP Command Example

The following example displays the IGMP status.

```
ras> ip igmp status
Group           groupLink           ifaceLink           flags
224.0.0.12      [0102fd80 00c618c0] [0102fdc4 0102fdc4] 0003
224.0.0.9       [0102fd4c 0102fdb4] [0102fd90 0102fd90] 0001
224.0.0.2       [0102fd18 0102fd80] [0102fd5c 0102fd5c] 0001
224.0.0.1       [00c618c0 0102fd4c] [0102fd28 0102fd28] 0001

iface enif0 flags 00000000
  query interval 125 sec, max rsp time 100 1/10 sec, group timeout 260 sec,
  counter 0, query timer 0 sec, v1 host present timer 0 sec,
  ttl threshold 1
  multicast group:
------------------snip----------------------
iface enif5:1 flags 00000000
  query interval 0 sec, max rsp time 0 1/10 sec, group timeout 0 sec,
  counter 0, query timer 0 sec, v1 host present timer 0 sec,
  ttl threshold 0
  multicast group:
```

The following table describes the labels in this display.

Table 53 ip igmp status Description

LABEL	DESCRIPTION
Group	This field displays group multicast IP addresses.
groupLink ifaceLink flags	These fields are for debug purposes. Send a screenshot of this screen to customer support if there are problems with IGMP snooping on the ZyWALL.
iface	This is the ZyWALL interface.
flags	00000000
query interval	This is the time period between sending IGMP Host Membership Queries.
max rsp time	This is the IGMP maximum response time.
group timeout	The IGMP group timeout.
counter	The IGMP counter.
query timer	This is how long a multicast router waits before deciding there is not another multicast router that should be the querier.
v1 host present timer	How long the ZyWALL waits to detect the presence of another IGMPv1 router.
ttl threshold	The IGMP group time to live threshold.
multicast group	This field lists any multicast groups to which the interface belongs.

15.1.16 NAT Commands

The following section lists the NAT commands.

Table 54 NAT Commands

COMMAND	DESCRIPTION	M
`ip nat hashtable <enifx>[`*`vpn-index`*`]`	Displays the NAT hash table of the specified Ethernet interface (or IP alias on an interface). `enif0`: The LAN interface. `enif1`: The WAN Ethernet interface. `enif2`: The DMZ interface. `enif3`: The WLAN interface.	R
`ip nat historicalCHigh`	Displays the current historical highest count of concurrent NAT sessions.	R
`ip nat historicalHigh`	Displays the current historical highest count of NAT sessions used by a single host.	R
`ip nat resetport`	Resets all NAT server table entries.	R
`ip nat routing [0:LAN|1:DMZ] [0:no|1:yes]`	Turns NAT routing on or off for the specified interface.	R
`ip nat server clear <`*`index`*`>`	Clears NAT port forwarding settings.	R
`ip nat server disp [`*`index`*`]`	Displays the NAT server table.	R
`ip nat server edit <`*`index`*`> active <yes|no>`	Turns the NAT port forwarding rule on or off.	R
`ip nat server edit <`*`index`*`> clear`	Clears the NAT port forwarding rule.	R
`ip nat server edit <`*`index`*`> forwardip <`*`ip-address`*`>`	Sets the IP address to which the NAT port forwarding rule forwards traffic.	R

Table 54 NAT Commands (continued)

COMMAND	DESCRIPTION	M
ip nat server edit <*index*> intport <*start-port*> [*end-port*]	Sets the port or port range the NAT port forwarding rule uses when forwarding traffic (port translation).	R
ip nat server edit <*index*> protocol <TCP|UDP|ALL>	Sets the NAT port forwarding rule's protocol.	R
ip nat server edit <*index*> remotehost <*start-ip*> [*end-ip*]	Sets the source IP address or IP address range for traffic to which the NAT port forwarding rule applies.	R
ip nat server edit <*index*> rulename <*name*>	Sets the name of the NAT port forwarding rule.	R
ip nat server edit <*index*> svrport <*start-port*> [*end-port*]	Sets the NAT port forwarding rule's listening (incoming) port or port range.	R
ip nat server load <*index*>	Loads the NAT port forwarding entry for editing.	R
ip nat server save	Saves NAT port forwarding settings to the non-volatile memory.	R
ip nat service aol [on|off]	Turns the AOL ALG on or off.	R
ip nat service irc [on|off]	Turns the IRC ALG on or off.	R
ip nat service ldap [on|off]	Turns the LDAP ALG on or off.	R
ip nat service xboxlive [on|off]	Turns the Xbox Live ALG on or off.	R
ip nat session [*sessions-per-host*]	Sets the allowed number of NAT sessions per host.	R

15.1.17 NAT Routing Command Example

Syntax: `ip nat routing [0:LAN|1:DMZ|2:WLAN] [0:no|1:yes]`

Use this command to set the ZyWALL to route traffic that does not match a NAT rule through a specific interface. An example of when you may want to use this is if you have servers with public IP addresses connected to the LAN, DMZ or WLAN. By default the ZyWALL routes traffic that does not match a NAT rule out through the DMZ interface.

The following command example sets the ZyWALL to route traffic that does not match a NAT rule through the WLAN interface.

```
ras> ip nat routing 2 1
Routing can work in NAT when no NAT rule match.
-----------------------------------------------
         LAN: no
         DMZ: yes
        WLAN: yes
```

15.1.18 Route Commands

The following section lists the route commands.

Table 55 Route Commands

COMMAND	DESCRIPTION	M
`ip route add <dest_address|default>[/<mask-bits>] <gateway-ip> [<metric>]`	Adds a route. The route is runtime only (it is not kept in non-volatile memory).	R
`ip route addiface <dest-ip-address>[/<mask-bits>] <interface> [<metric>]`	Adds an entry to the routing table for the specified interface.	R
`ip route drop <ip-address> [/<mask-bits>]`	Drops a route.	R
`ip route status`	Displays the routing table.	R

15.1.19 Report and Status Commands

The following section lists the report and status commands.

Table 56 Report and Status Commands

COMMAND	DESCRIPTION	M
`ip rpt active [0:no|1:yes]`	Enables or disables the system reports.	R+B
`ip rpt ip [0:lan|1:dmz] [number]`	Displays the IP addresses (connected to the specified interface) that sent and received the most traffic.	R+B
`ip rpt srv [0:lan|1:dmz] [number]`	Displays the most heavily used protocols or service ports.	R+B
`ip rpt start [0:lan|1:dmz]`	Starts recording reports data for the specified port’s traffic.	R+B
`ip rpt stop [0:lan|1:dmz]`	Stops recording reports data for the specified port’s traffic.	R+B
`ip rpt url [0:lan|1:dmz] [number]`	Displays the specified port’s most visited Web sites.	R+B
`ip status`	Displays IP statistic counters.	R+B
`ip tcp status`	Displays the TCP statistics counters.	R+B
`ip udp status`	Displays the UDP status.	R+B

15.1.20 Static Route Commands

The following section lists the static route commands.

Table 57 Static Route Commands

COMMAND	DESCRIPTION	M
`ip stroute config active <yes|no>`	Enables or disables a static route rule. You must use the load command before you can configure a static route.	R
`ip stroute config destination <dest-ip-address>[/<mask-bits>] <gateway-ip> [<metric>]`	Sets a static route’s destination IP address and gateway.	R
`ip stroute config gateway <ip>`	Sets a static route’s gateway IP address.	R
`ip stroute config mask <mask>`	Sets a static route’s subnet mask.	R

Table 57 Static Route Commands (continued)

COMMAND	DESCRIPTION	M
ip stroute config metric <*metric*>	Sets a static route’s metric number.	R
ip stroute config name <*site-name*>	Sets the name for a static route.	R
ip stroute display [*index*|buf]	Displays the list of static routes or detailed information on a specified rule.	R
ip stroute load <*index*>	Loads the specified static route rule for editing.	R
ip stroute save	Saves a rule in the non-volatile memory.	R

15.1.21 Static Route Command Example

The following example configures a static route named Example that sends all traffic for IP address 2.2.2.2 to a gateway at 192.168.1.9 and has a metric of 3.

```
ras> ip stroute load 3
========== Routing Rule in Buffer ==========
Route number : 3
Route Name :
Active : No
Destination IP Address : 0.0.0.0
IP Subnet Mask : 0.0.0.0
Gateway IP Address : 0.0.0.0
Metric : 0
Private : No
ras> ip stroute config name Example
Change Route Name to : Example
ras> ip stroute config destination 2.2.2.2 192.168.1.9 3
Change Destination IP Address to : 2.2.2.2
Change Gateway IP Address to : 192.168.1.9
Change Subnet Mask to : 255.0.0.0
ras> ip stroute config active yes
Setting Active to Yes.
ras> ip stroute save
=========== Routing Rule Setting ===========
Route number : 3
Route Name : Example
Active : Yes
Destination IP Address : 2.2.2.2
IP Subnet Mask : 255.0.0.0
Gateway IP Address : 192.168.1.9
Metric : 3
Private : No
```

15.1.22 Traffic Redirect Commands

The following section lists the traffic redirect commands.

Table 58 Traffic Redirect Commands

COMMAND	DESCRIPTION	M
`ip tredir active <on|off>`	Enables or disables traffic redirect.	R
`ip tredir checktime <period>`	Sets the number of seconds (0~255) ZyWALL waits between attempts to connect to the target.	R
`ip tredir disp`	Displays the traffic redirect configuration.	R
`ip tredir failcount <count>`	Sets the number of times that ZyWALL can ping the target without a response before forwarding traffic to the backup gateway.	R
`ip tredir partner <ip-address>`	Sets the traffic redirect backup gateway IP address.	R
`ip tredir save`	Saves traffic redirect configuration.	R
`ip tredir target <ip-address>`	Sets the IP address that ZyWALL uses to test WAN accessibility.	R
`ip tredir timeout <timeout>`	Sets the maximum number of seconds (0~255) ZyWALL waits for a response from the target.	R

15.1.23 Other IP Commands

The following section lists miscellaneous IP commands.

Table 59 Other ip Commands

COMMAND	DESCRIPTION	M
`ip aliasdis <0|1>`	Disables or enables routing between the alias networks.	R
`ip dropFrag [on|off]`	Turn on this command to have the ZyWALL drop IP fragment packets. The ZyWALL does not save the setting for this command in the non-volatile memory.	R+B
`ip dropIcmp [0|1]`	Sets whether or not the ZyWALL drops ICMP fragment packets.	R+B
`ip ident [on|off]`	Turn on this command to have the ZyWALL drop identification protocol packets (RFC 1413).	R+B
`ip ifconfig [interface] [ip-address</mask-bits>] <broadcast [address]> <mtu [value]> <mss [value]> <dynamic> <showoff>`	Configures a network interface. `mtu`: Sets the Maximum Transmission Unit. `mss`: Sets the Maximum Segment Size. `dynamic`: Sets the interface to get an IP address via DHCP. `showoff`: Turns off the interface.	R+B
`ip ping <address>`	Pings a remote host IP address or domain name.	R+B

Table 59 Other ip Commands (continued)

COMMAND	DESCRIPTION	M
ip pingext [*target address*] [-n] [*repeat-value*] [-l] [*data-size*] [-w] [*timeout-value*] [-o] [*ip-address|interface*] [-v] [*tos-value*] [-c][-d] [*data*] [-f] [-p] [*min-mtu*] [*max-mtu*] [*interval-size*]	Pings a remote host. -c : Validate the reply data. -d *data* : Data pattern. The maximum length of data is 255 characters. -f : Set DF flag. -l *data-size* : Datagram size in bytes (with 28 bytes Header). -v *tos-value* : Specify the value of TOS flag. -n *repeat-value* : The number of times to send a ECHO_REQ packet. -w *timeout-value*: Specify the value of Timeout in seconds. -o *ip-address|interface*: Specify one IP address or interface to be the source IP address. -p *min-mtu max-mtu interval-size*: Sweep range of sizes.	R
ip telnet <*address*> [*port*]	Creates a Telnet connection to the specified host.	R+B
ip traceroute <*address*> [*ttl*] [*wait*] [*queries*]	Sends ICMP packets to trace the route of a remote host. *ttl*: Time to live in seconds (0~255). *wait*: Timeout in seconds (0~255). *queries*: The number of ICMP packets to use (1~5).	R+B

15.1.24 Interface Command Example

The following example sets the WAN 1 interface to use IP address 172.16.2.2 and subnet mask 255.255.0.0.

```
ras> ip ifconfig enif1 172.16.2.2/16
enif1: mtu 1500 mss 1460
    inet 172.16.2.2, netmask 0xffff0000, broadcast 172.16.255.255
    RIP RX:None, TX:None,
    [InOctets        197396] [InUnicast       621] [InMulticast          982]
    [InDiscards          72] [InErrors          0] [InUnknownProtos       72]
    [OutOctets        89305] [OutUnicast      629] [OutMulticast           0]
    [OutDiscards          0] [OutErrors         0]
```

15.1.25 Ping Command Example

The following command has the ZyWALL ping IP address 172.16.2.56 5 times.

```
ras> ip pingext 172.16.2.56 -n 5
Resolving 172.16.2.56... 172.16.2.56
      sent      rcvd    size     rtt     avg     max     min
         1         1      36       0       0       0       0
         2         2      36       0       0       0       0
         3         3      36       0       0       0       0
         4         4      36       0       0       0       0
         5         5      36       0       0       0       0

Extended Ping From device to 172.16.2.56:
   Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate Round Trip Times in milli-seconds:
   RTT: Average = 0ms, Maximum =  0ms, Minimum = 0ms
```

16

IPSec Commands

Use these commands to configure IPSec settings on the ZyWALL.

16.1 Command Summary

The following table describes the values required for many commands. Other values are discussed with the corresponding commands.

Table 60 BM Class Command Input Values

LABEL	DESCRIPTION
`<interface>`	This is an interface name including lan, wan/wan1, dmz, wan2, wlan.

The following section lists the commands for this feature.

Table 61 Ipsec Commands

COMMAND	DESCRIPTION	M
`ipsec debug type <0:Disable|1:Original <on|off>|2:IKE <on|off>|3:IPSec [SPI] <on|off>|4:XAUTH <on|off>|5:CERT <on|off>|6:All>`	Controls whether the specified debugging information is displayed on the console.	R+B
`ipsec debug level <0:None|1:User|2:Low|3:High>`	Sets the debugging level. The higher the number specified, the more detail displays.	R+B
`ipsec debug display`	Displays all debugging settings.	R+B
`ipsec route <interface> [on|off]`	After IPSec processes a packet that will be sent to the specified interface, this switch controls whether or not the packets can be forwarded to another IPSec tunnel.	R
`ipsec show_runtime sa`	Displays active IKE and IPSec SAs.	R+B
`ipsec show_runtime spd`	Displays the local and remote network address pairs used to differentiate the connected dynamic VPN tunnels.	R+B
`ipsec show_runtime list`	Displays active VPN tunnels.	R+B
`ipsec timer chk_conn <time>`	The ZyWALL disconnects a VPN tunnel if there is no reply traffic for this number of minutes. This is also called the output idle timer. *time*: 120~3600 seconds. The default is 120 seconds.	R+B

Table 61 Ipsec Commands (continued)

COMMAND	DESCRIPTION	M
`ipsec timer update_peer <time>`	For IPSec rules with a domain name as the local or remote gateway address, this command sets the interval (in minutes) for resolving the domain name and updating the rules. *time*: 2~60 minutes. The default is 5 minutes. 0 disables the updates.	R+B
`ipsec timer chk_input <time>`	The ZyWALL disconnects any IPSec connection that has no inbound traffic for this number of seconds. This is also called the input idle timer. *time*: 30~3600 seconds. `0` disables the check (this is the default setting).	R+B
`ipsec updatePeerIp`	If you use a domain name as the local or remote gateway address, this command forces the ZyWALL to resolve the domain name and update the IPSec rules right away.	R+B
`ipsec dial <policy index>`	Dials the specified IPSec policy # manually.	R+B
`ipsec enable [on|off]`	Enables or disables all IPSec rules.	R+B
`ipsec ikeDisplay <rule-number>`	Displays the specified IKE rule. Or displays all runtime IKE rules without specifying a rule. Use ikeAdd or ikeEdit to load an IKE rule before using this command.	R+B
`ipsec ikeAdd`	Allocates a working buffer to add an IKE rule.	R+B
`ipsec ikeEdit <rule-number>`	Loads the specified IKE rule for editing.	R+B
`ipsec ikeSave`	Saves the IKE rule settings from buffer to memory.	R+B
`ipsec ikeList`	Lists all IKE rules.	R+B
`ipsec ikeDelete <rule-number>`	Deletes the specified IKE rule.	R+B
`ipsec ikeConfig name <string>`	Sets the IKE rule name. *string*: Up to 31 characters.	R+B
`ipsec ikeConfig negotiationMode <0:Main|1:Aggressive>`	Sets the negotiation mode.	R+B
`ipsec ikeConfig natTraversal <Yes|No>`	Turns NAT traversal on or off.	R+B
`ipsec ikeConfig multiPro <Yes|No>`	Turns multiple proposal on or off.	R+B
`ipsec ikeConfig lcIdType <0:IP|1:DNS|2:Email>`	Sets the local ID type.	R+B
`ipsec ikeConfig lcIdContent <content>`	Sets the local ID content with the specified IP address, domain name, or e-mail address. Use up to 31 characters.	R+B
`ipsec ikeConfig myIpAddr <ip-address|domain-name>`	Sets the local VPN gateway with the specified IP address or domain name.	R
`ipsec ikeConfig peerIdType <0:IP|1:DNS|2:Email>`	Sets the peer ID type.	R+B
`ipsec ikeConfig peerIdContent <string>`	Sets the peer ID content with the specified IP address, domain name, or e-mail address. Use up to 31 characters.	R+B
`ipsec ikeConfig secureGwAddr <ip-address|domain-name>`	Sets the remote gateway address with the specified IP address or domain name.	R+B

Table 61 Ipsec Commands (continued)

COMMAND	DESCRIPTION	M
`ipsec ikeConfig authMethod <0:PreSharedKey|1:RSASignature|2:preShareKey+XAUTH|3:RSASignature+XAUTH>`	Sets the authentication method.	R+B
`ipsec ikeConfig preShareKey` *<ascii|0xhex>*	Sets the pre-shared key. *ascii|0xhex*: Enter characters in ASCII or in hexadecimal format. The minimum length is 8.	R+B
`ipsec ikeConfig certificate` *<certificate-name>*	Specifies the certificate the ZyWALL uses for authentication.	R+B
`ipsec ikeConfig encryAlgo <0:DES|1:3DES|2:AES>`	Sets the phase 1 encryption algorithm.	R+B
`ipsec ikeConfig authAlgo <0:MD5|1:SHA1>`	Sets the phase 1 authentication algorithm.	R+B
`ipsec ikeConfig saLifeTime` *<seconds>*	Sets the phase 1 IKE SA life time.	R+B
`ipsec ikeConfig keyGroup <0:DH1|1:DH2>`	Sets the phase 1 IKE SA key group.	R+B
`ipsec ikeConfig xauth type <0:client mode|1:server mode>`	Sets the ZyWALL in client or server mode for extended authentication (Xauth).	R+B
`ipsec ikeConfig xauth username` *<name>*	Sets the user name for Xauth. This uses the ZyWALL's local user database to authenticate the remote user.	R+B
`ipsec ikeConfig xauth password` *<password>*	Sets the password for Xauth.	R+B
`ipsec ikeConfig xauth radius` *<username> <password>*	Sets the RADIUS server user name and password.	R+B
`ipsec ikeConfig ha enable <on|off>`	Enables IPSec high availability (HA).	R+B
`ipsec ikeConfig ha redunSecGwAddr` *<ip-address|domain-name>*	Sets the redundant remote gateway address to the specified IP address or domain name.	R+B
`ipsec ikeConfig ha fallback enable <on|off>`	Enables fall back for IPSec HA.	R+B
`ipsec ikeConfig ha fallback interval` *<time>*	Enables a time interval for how often the ZyWALL checks the availability of primary remote gateway for fall back detection. *time*: 180~86400 seconds	R+B
`ipsec ikeConfig ha failover display`	Displays fail over detection method.	R+B
`ipsec ikeConfig ha failover dpd <on|off>`	Enables or disables fail over detection by Dead Peer Detection (DPD).	R+B
`ipsec ikeConfig ha failover outputIdleTime <on|off>`	Enables or disables fail over detection by output idle timer. If the time is up and there is no reply traffic, the ZyWALL disconnects the tunnel and negotiates a new tunnel with the redundant remote VPN gateway.	R+B
`ipsec ikeConfig ha failover pingCheck <on|off>`	Enables or disables fail over detection by ping check. If the ZyWALL cannot ping the pre-configured IP address for several retries, the ZyWALL disconnects the tunnel and negotiates a new tunnel with the redundant remote VPN gateway.	R+B

Table 61 Ipsec Commands (continued)

COMMAND	DESCRIPTION	M
`ipsec ipsecDisplay <rule-number>`	Displays the specified IPSec rule. Or displays all runtime IPSec rules without specifying a rule. Use ipsecAdd or ipsecEdit to load an IPSec rule before using this command.	R+B
`ipsec ipsecAdd`	Allocates a working buffer to add an IPSec rule.	R+B
`ipsec ipsecEdit <rule-number>`	Loads the specified IPSec rule for editing.	R+B
`ipsec ipsecSave`	Saves the IPSec rule settings from the working buffer to the non-volatile memory.	R+B
`ipsec ipsecList`	Lists all IPSec rules.	R+B
`ipsec ipsecDelete <rule-number>`	Deletes the specified IPSec rule.	R+B
`ipsec ipsecConfig name <name>`	Sets the IPSec rule's name (up to 31 characters).	R+B
`ipsec ipsecConfig active <Yes|No>`	Turns the IPSec rule on or off.	R+B
`ipsec ipsecConfig saIndex <index>`	Binds the IPSec rule with the specified IKE rule.	R+B
`ipsec ipsecConfig multiPro <Yes|No>`	Enables the multiple proposal.	R+B
`ipsec ipsecConfig nailUp <Yes|No>`	Enables the nailed-up.	R+B
`ipsec ipsecConfig activeProtocol <0:AH|1:ESP>`	Sets the active protocol.	R+B
`ipsec ipsecConfig encryAlgo <0:Null|1:DES| 2:3DES|3:AES>`	Sets the phase 2 encryption algorithm.	R+B
`ipsec ipsecConfig encryKeyLen <0:128|1:192|2:256>`	Sets the phase 2 encryption key length.	R+B
`ipsec ipsecConfig authAlgo <0:MD5|1:SHA1>`	Sets the phase 2 authentication algorithm.	R+B
`ipsec ipsecConfig saLifeTime <seconds>`	Sets the phase 2 IPSec SA life time.	R+B
`ipsec ipsecConfig encap <0:Tunnel|1:Transport>`	Sets the phase 2 encapsulation mode.	R+B
`ipsec ipsecConfig pfs <0:None|1:DH1|2:DH2>`	Sets the Perfect Forward Secrecy group for phase 2.	R+B
`ipsec ipsecConfig antiReplay <Yes|No>`	Enables or disables replay detection.	R+B
`ipsec ipsecConfig controlPing <Yes|No>`	Enables or disables the IPSec tunnel connectivity check.	R+B
`ipsec ipsecConfig logControlPing <Yes|No>`	Enables or disables logging for the ping check events including pings sent and responses.	R+B
`ipsec ipsecConfig controlPingAddr <ip-address>`	Sets the destination address for ping check.	R+B
`ipsec ipsecConfig protocol <1:ICMP|6:TCP|17:UDP>`	Sets the traffic protocol that can trigger the VPN tunnel and be forwarded through it.	R+B
`ipsec ipsecConfig lcAddrType <0:single|1:range|2:subnet>`	Sets the address type for the local network.	R+B
`ipsec ipsecConfig lcAddrStart <ip-address>`	Sets the local network starting IP address.	R+B
`ipsec ipsecConfig lcAddrEndMask <ip-address|subnet-mask>`	Sets the local network ending IP address for a range or the subnet mask for a subnet.	R+B

Table 61 Ipsec Commands (continued)

COMMAND	DESCRIPTION	M
ipsec ipsecConfig lcPortStart <*port*>	Sets the starting port for local network traffic. Only traffic using the specified ports can go through the VPN tunnel.	R+B
ipsec ipsecConfig lcPortEnd <*port*>	Sets the ending port for local network traffic.	R+B
ipsec ipsecConfig rmAddrType <0:single|1:range|2:subnet>	Sets the address type for the remote network.	R+B
ipsec ipsecConfig rmAddrStart <*ip-address*>	Sets the remote network starting IP address.	R+B
ipsec ipsecConfig rmAddrEndMask <*ip-address*|*subnet-mask*>	Sets the remote network ending IP address for a range or the subnet mask for a subnet.	R+B
ipsec ipsecConfig rmPortStart <*port*>	Sets the starting port for remote network traffic. Only traffic using the specified ports can go through the VPN tunnel.	R+B
ipsec ipsecConfig rmPortEnd <*port*>	Sets the ending port for remote network traffic.	R+B
ipsec ipsecConfig activeZero <Yes|No>	Turns Zero Configuration mode on or off.	R+B
ipsec ipsecConfig natActive <Yes|No>	Turns NAT over IPSec on or off.	R+B
ipsec ipsecConfig natType <0:One-to-One|1:Many-to-One|2:Many-One-to-One>	Sets the NAT mapping types.	R+B
ipsec ipsecConfig natPrivateStart <*ip-address*>	Sets the private network starting IP address when you enable NAT over IPSEC.	R+B
ipsec ipsecConfig natPrivateEnd <*ip-address*>	Sets the private network ending IP address when you enable NAT over IPSEC.	R+B
ipsec policyList	Lists all IPSec policy rules.	R+B
ipsec manualDisplay <*rule-number*>	Displays the specified manual rule. Or displays all runtime manual rules without specifying a rule. Use manualAdd or manualEdit to load a manual rule before using this command.	R+B
ipsec manualAdd	Allocates a working buffer to add an manual rule.	R+B
ipsec manualEdit <*rule-number*>	Loads the specified manual rule for editing.	R+B
ipsec manualSave	Saves the manual rule settings from the working buffer to the non-volatile memory.	R+B
ipsec manualList	Lists all manual rules.	R+B
ipsec manualDelete <*rule-number*>	Deletes the specified manual rule.	R+B
ipsec manualConfig name <*string*>	Sets the manual rule name. <*string*>: Up to 31 characters.	R+B
ipsec manualConfig active <Yes|No>	Activates the manual rule.	R+B
ipsec manualConfig myIpAddr <*ip-address*|*domain-name*>	Sets the local gateway address to the specified IP address or domain name.	R
ipsec manualConfig secureGwAddr <*ip-address*|*domain-name*>	Sets the remote gateway address to the specified IP address or domain name.	R+B
ipsec manualConfig protocol <1:ICMP|6:TCP|17:UDP>	Sets the traffic protocol that can trigger the VPN tunnel and be forwarded through it.	R+B
ipsec manualConfig lcAddrType <0:single|1:range|2:subnet>	Sets the local address type.	R+B

Table 61 Ipsec Commands (continued)

COMMAND	DESCRIPTION	M
`ipsec manualConfig lcAddrStart <ip-address>`	Sets the local network starting IP address.	R+B
`ipsec manualConfig lcAddrEndMask <ip-address>`	Sets the local network ending IP address for a range or the subnet mask for a subnet.	R+B
`ipsec manualConfig lcPortStart <port>`	Sets the starting port for local network traffic. This is to limit the traffic sent or received in the VPN tunnel.	R+B
`ipsec manualConfig lcPortEnd <port>`	Sets the ending port for local network traffic. This is to limit the traffic sent or received in the VPN tunnel.	R+B
`ipsec manualConfig rmAddrType <0:single|1:range|2:subnet>`	Sets the remote address type.	R+B
`ipsec manualConfig rmAddrStart <ip-address>`	Sets the remote network starting IP address.	R+B
`ipsec manualConfig rmAddrEndMask <ip-address>`	Sets the remote network ending IP address for a range or the subnet mask for a subnet.	R+B
`ipsec manualConfig rmPortStart <port>`	Sets the starting port for remote network traffic. This is to limit the traffic sent or received in the VPN tunnel.	R+B
`ipsec manualConfig rmPortEnd <port>`	Sets the ending port for remote network traffic. This is to limit the traffic sent or received in the VPN tunnel.	R+B
`ipsec manualConfig activeProtocol <0:AH|1:ESP>`	Sets the protocol the manual key rule uses.	R+B
`ipsec manualConfig ah encap <0:Tunnel|1:Transport>`	Sets the encapsulation mode when using AH protocol in the manual rule.	R+B
`ipsec manualConfig ah spi <decimal>`	Sets the SPI information when using AH protocol in the manual rule. *decimal*: The maximum length is 9.	R+B
`ipsec manualConfig ah authAlgo <0:MD5|1:SHA1>`	Sets the authentication algorithm when using AH protocol in the manual rule.	R+B
`ipsec manualConfig ah authKey <ascii>`	Sets the authentication key when using AH protocol in the manual rule.	R+B
`ipsec manualConfig esp encap <0:Tunnel|1:Transport>`	Sets the encapsulation mode when using ESP protocol in the manual rule.	R+B
`ipsec manualConfig esp spi <decimal>`	Sets the SPI when using ESP protocol in the manual rule. *decimal*: The maximum length is 9.	R+B
`ipsec manualConfig esp encryAlgo <0:Null|1:DES|2:3DES>`	Sets the encryption algorithm when using ESP protocol in the manual rule.	R+B
`ipsec manualConfig esp encryKey <string>`	Sets the encryption key when using ESP protocol in the manual rule.	R+B
`ipsec manualConfig esp authAlgo <0:MD5|1:SHA1>`	Sets the authentication algorithm when using ESP protocol in the manual rule.	R+B
`ipsec manualConfig esp authKey <string>`	Sets the authentication key when using ESP protocol in the manual rule.	R+B
`ipsec manualPolicyList`	Lists all manual policy rules.	R+B
`ipsec CRYPTIC_1141 <on|off>`	Turns one of the ZyWALL's hardware VPN accelerators on or off.	R+B

Table 61 Ipsec Commands (continued)

COMMAND	DESCRIPTION	M
`ipsec swSkipOverlapIp <on|off>`	Turn this on to send packets destined for overlapping local and remote IP addresses to the local network (you can access the local devices but not the remote devices). Turn this off to send packets destined for overlapping local and remote IP addresses to the remote network (you can access the remote devices but not the local devices.)	R+B
`ipsec swCfScan <on|off>`	Enables or disables content filtering for IPSec packets.	R+B
`ipsec adjTcpMss <off|auto|`*`user-defined-value`*`>`	The TCP packets are larger after VPN encryption. Packets larger than a connection's MTU (Maximum Transmit Unit) are fragmented. `auto`: Automatically set the Maximum Segment Size (MSS) of the TCP packets that are to be encrypted by VPN based on the encapsulation type. Recommended. *`user-defined-value`*: If fragmentation issues are affecting your network's throughput performance, you can manually specify a smaller MSS (1~1460 bytes).	R+B
`ipsec ha debug <on|off|runtime|spt>`	Controls whether the HA debugging information is displayed or not on console. Sets the runtime or spt with the command to display runtime data or the data stored in the ZyWALL's non-volatile memory.	R+B
`ipsec Drop <`*`policy-index`*`>`	Disconnects the specified tunnel.	R+B
`ipsec swSkipPPTP <on|off>`	Set on to not forward PPTP packets to an IPSec tunnel.	R+B
`ipsec initContactMode <tunnel|gateway>`	Enables initial contact based on tunnel or gateway mode. In gateway mode, the ZyWALL would disconnect all tunnels behind a same NAT router after receiving a notify of initial contact. In the same case, the ZyWALL just disconnect one tunnel.	R
`ipsec pingCheckDropEnable <on|off>`	Turn this on to drop a tunnel if the number of VPN ping check packet retries reaches its limit, even when VPN HA is not enabled. Turn this off to have the device only do this when VPN HA is enabled.	R+B
`ipsec pingPeriod <10-600>`	Sets how many seconds the ZyWALL waits for a reply to a VPN ping check before dropping the tunnel.	R+B
`ipsec pingRetryCnt <1-10>`	Sets the number of retries for a VPN ping check.	R+B
`ipsec swDevTri <on|off>`	Enables the ZyWALL to forward traffic from itself through a VPN tunnel. The traffic includes time zone update, AV/IDP signature updates, WAN connectivity ping checks, VPN connectivity ping checks, and remote management.	R+B

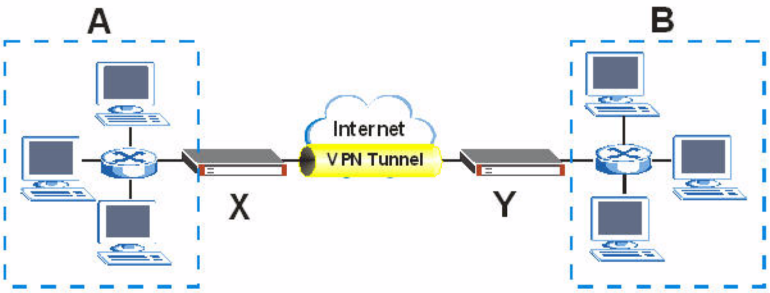
16.2 swSkipOverlapIp

Normally, we don't configure the local VPN policy rule’s IP addresses to overlap with the remote VPN policy rule’s IP addresses. For example, we don't configure both with 192.168.1.0. However, overlapping local and remote network IP addresses can occur in the following cases.

1 You configure a dynamic VPN rule for a remote site. (See Figure 4 on page 128.)

For example, when you configure the ZyWALL X, you configure the local network as 192.168.1.0 and the remote network as any (0.0.0.0). The “any” includes all possible IP addresses. It will forward traffic from network A to network B even if both the sender (ex. 192.168.1.8) and the receiver (ex. 192.168.1.9) are in network A.

Figure 4 Dynamic VPN Rule



Using the command `ipsec swSkipOverlapIp on` has ZyWALL X check if a packet’s destination is also at the local network before forwarding the packet. If it is, the ZyWALL sends the traffic to the local network. Setting `ipsec swSkipOverlapIp` to `off` disables the checking for local network IP addresses.

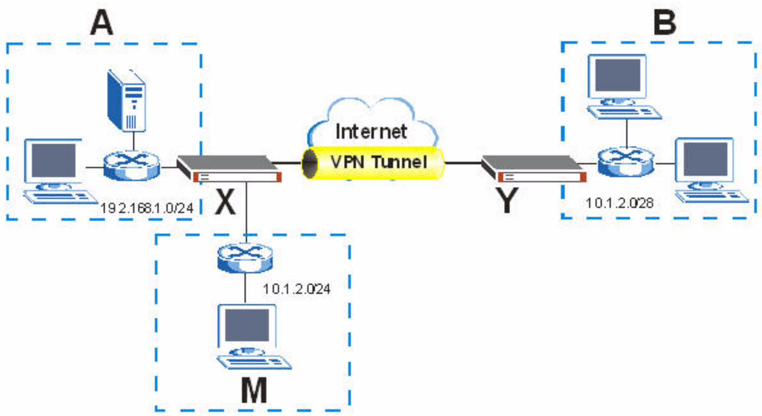
2 You configure an IP alias network that overlaps with the VPN remote network. (See Figure 5.)

For example, you have an IP alias network M (10.1.2.0/24) in ZyWALL X’s LAN. For the VPN rule, you configure the VPN network as follows.

- Local IP address start: 192.168.1.1, end: 192.168.1.254
- Remote IP address start: 10.1.2.240, end: 10.1.2.254

IP address 10.1.2.240 to 10.1.2.254 overlap.

Figure 5 IP Alias

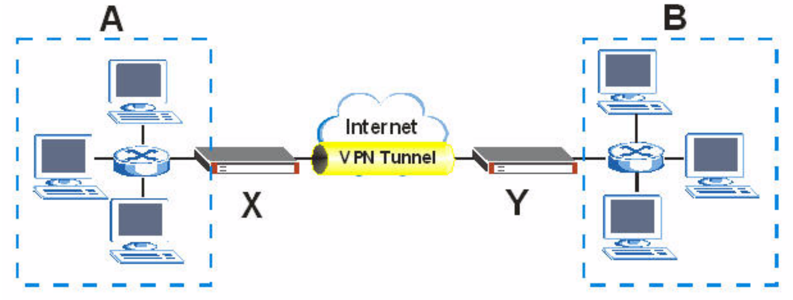


In this case, if you want to send packets from network A to an overlapped IP (ex. 10.1.2.241) that is in the IP alias network M, you have to set the `swSkipOverlapIp` command to `on`.

16.3 Detect Zombie Tunnels in Tunnel or Gateway Mode

The initial contact feature detects zombie tunnels and re-establishes them right away. For example, in Figure 6, the ZyWALL X will have a zombie tunnel if ZyWALL Y suddenly turns off. ZyWALL X still tries to send traffic through the VPN tunnel. When ZyWALL Y turns back on, it may have a new IP when it tries to establish the tunnel with ZyWALL X. Enabling the initial contact feature on ZyWALL X makes the ZyWALL X delete the zombie tunnel upon receiving the initial contact from ZyWALL Y and establish a new tunnel.

Figure 6 Initial Contact example 1



In addition, assume there are three VPN tunnels using the two VPN gateways. See Figure 7.

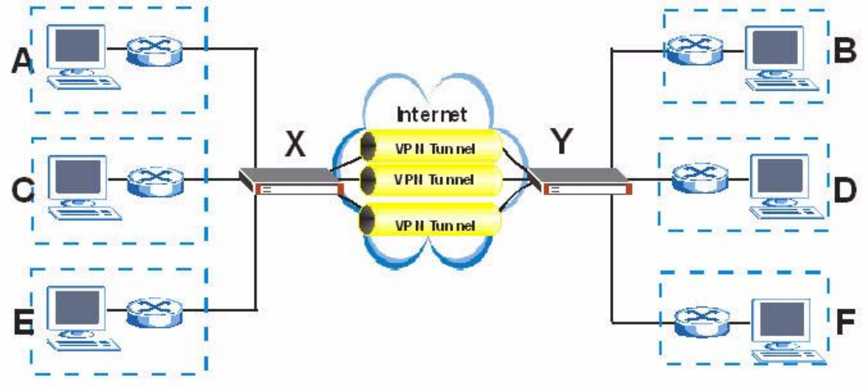
VPN tunnel 1: Local network: A, Remote network: B.

VPN tunnel 2: Local network: C, Remote network: D.

VPN tunnel 3: Local network: E, Remote network: F.

- When you use `ipsec initContactMode gateway`, the initial contact sent from network B makes the ZyWALL X remove all three tunnels and re-build new ones.
- When you use `ipsec initContactMode tunnel`, the initial contact sent from network B makes the ZyWALL X remove and re-build only tunnel 1.

Figure 7 Initial Contact Example 1



16.4 Command Examples

This example adds an IKE rule as follows.

- IKE Rule Name: VPN-ph1
- My IP Address: 10.1.1.1
- Secure Gateway Address: 10.1.1.2
- Authentication: Pre-Shared Key
- Pre-Shared Key: 12345678

```
ras> ipsec ikeAdd
ras> ipsec ikeConfig name VPN-ph1
ras> ipsec ikeConfig myIpAddr 10.1.1.1
ras> ipsec ikeConfig secureGwAddr 10.1.1.2
ras> ipsec ikeConfig authMethod 0
ras> ipsec ikeConfig preShareKey 12345678
ras> ipsec ikeSave
```

This example enables VPN HA on an existing IKE rule.

You need to load an IKE rule first by ikeAdd or ikeEdit before you configure IKE settings.

- IKE Rule index: 1
- The redundant secure gateway IP: 10.1.1.5
- Fall back detection: Enable
- The time interval for fall back detection: 180 seconds
- DPD for fail over detection: Enable
- Output idle Timeout for fail over detection: Enable

```
ras> ipsec ikeList
Configure IKE number 1
Idx SPD Name                 Flags MyIP            SecureGW
===============================================================================
  1   0 VPN-ph1                  3 10.1.1.1         10.1.1.2
ras> ipsec ikeEdit 1
ras> ipsec ikeConfig ha enable on
ras> ipsec ikeConfig ha redunSecGwAddr 10.1.1.5
ras> ipsec ikeConfig ha fallback enable on
ras> ipsec ikeConfig ha fallback interval 180
ras> ipsec ikeConfig ha failover dpd on
ras> ipsec ikeConfig ha failover outputIdleTime on
ras> ipsec ikeConfig ha failover display
Fail over detection methods:
Output Idle Time: Yes
DPD: Yes
Ping Check: No
ras> ipsec ikeSave
```

This example adds an IPSec rule as follows.

1. The IPSec Rule Index: 1
2. Rule Name: VPN-ph2
3. Active
4. Link the IPSec settings with which IKE index rule: 1
5. The VPN protocol: ESP
6. Local Network Type: Subnet
7. Local Network Address Start: 192.168.1.0
8. Local Network Address End: 255.255.255.0
9. Remote Network Type: Single
10. Remote Network Address: 192.168.2.250
11. Key Management: IKE
12. Negotiation Mode: Main
13. Authentication Method: Pre-Shared Key
14. Pre-Shared Key: 12345678

```
ras> ipsec ipsecAdd
ras> ipsec ipsecConfig name VPN-ph2
ras> ipsec ipsecConfig active Yes
ras> ipsec ipsecConfig saIndex 1
ras> ipsec ipsecConfig activeProtocol 1
ras> ipsec ipsecConfig encap 0
ras> ipsec ipsecConfig lcAddrType 2
ras> ipsec ipsecConfig lcAddrStart 192.168.1.1
ras> ipsec ipsecConfig lcAddrEndMask 255.255.255.0
ras> ipsec ipsecConfig rmAddrType 0
ras> ipsec ipsecConfig rmAddrStart 192.168.2.250
ras> ipsec ipsecSave
```

17

Load Balancing Commands

Use these commands to configure load sharing (load balancing) settings on the ZyWALL.

17.1 Command Summary

The following section lists the load sharing commands.

Table 62 Load Balancing Commands

COMMAND	DESCRIPTION	M
`ls band <up|down> <wan1-bandwidth wan2-bandwidth>`	Configures Least Load First load balancing to measure upstream or downstream traffic and how many Kbps to distribute to each WAN interface.	R
`ls disp`	Displays the load balancing configuration.	R
`ls hostBase enable [0:disable|1:enable]`	Enables or disables the WAN Interface to local host mapping timeout. Enable it to have the ZyWALL send all of a local computer's traffic through the same WAN interface for the period of time that you specify using the `ls hostBase timeout` command.	
`ls hostBase runtime`	Displays whether WAN Interface to local host mapping is enabled or disabled.	
`ls hostBase timeout <1~600>`	Sets the timeout value for WAN Interface to local host mapping (1~600 seconds).	
`ls mode <1:LLF|2:WRR|3:Spillover|255:None>`	Sets the load balancing method. 1: Least Load First (dynamic load balancing) 2: Weighted Round Robin 3: Spillover. 255: disable load balancing	R
`ls spillover <bandwidth>`	Configures the spillover upper bandwidth of the primary WAN. For example, "ls spillover 100" has the ZyWALL send traffic to the secondary WAN when the primary WAN bandwidth exceeds 100 Kbps.	R
`ls timeframe <10~600>`	With Least Load First or spillover load balancing, set the ZyWALL to measure bandwidth using the average bandwidth during the specified time interval (10~600 seconds).	R
`ls wrr <wan1-weight> <wan2-weight>`	Configures the Weighted Round Robin weight parameters for the WAN1 and WAN2 interfaces. The weight can be 0~10.	R

17.2 Command Examples

This example sets Least Load First load balancing to distribute 100 Kbps of upstream traffic to WAN1 for every 200 Kbps of upstream traffic that goes through WAN2. The bandwidth measurement is averaged over 30 seconds. Then it changes the load balancing method to Least Load First.

```
ras> ls band up 100 200
ras> ls mode 1
ras> ls disp
Load Sharing Active: Yes
Load Sharing dispatch outgoing traffic by Least Load First
Method: Upstream
Upload traffic WAN1: 100, WAN2: 200
Download traffic WAN1: 0, WAN2: 0
ras> ls timeframe 30
```

This example configures Weighted Round Robin load balancing to give a weight of 10 to WAN1 and a weight of 5 to WAN2. Then it changes the load balancing method to Weighted Round Robin.

```
ras> ls wrr 10 5
ras> ls mode 2
ras> ls disp
Load Sharing Active: Yes
Load Sharing dispatch outgoing traffic by Weighted Round Robin
WAN1 weight: 10, WAN2 weight: 5
```

This example configures spillover load balancing to send traffic to the secondary WAN when the primary WAN bandwidth exceeds 100 Kbps. Then it changes the load balancing method to spillover.

```
ras> ls spillover 100
ras> ls mode 3
ras> ls disp
Load Sharing Active: Yes
Load Sharing dispatch outgoing traffic by Spillover
Send traffic to secondary WAN when primary WAN bandwidth exceeds 100 Kbps.
```

18

myZyXEL.com Commands

Use these commands to configure user, product, or service registration settings on your ZyWALL. Your ZyWALL needs to connect to the registration server (default is http://www.myZyXEL.com).

Ensure your **ZyWALL** is connected to the Internet and the registration server before you use the following commands.

18.1 Command Summary

The following section lists the commands for this feature.

Table 63 MyZyXEL Commands

COMMAND	DESCRIPTION	M
`sys myZyxelCom checkUserName <username>`	Checks whether the specified user name exists or not in the myZyXEL.com database.	R
`sys myZyxelCom register <username> <password> <email> <countrycode>`	Sends the specified registration information to myZyXEL.com including user name, password, email, and country code. *countrycode*: This is a number that represents the country you are from. Refer to table Table 64 on page 136.	R
`sys myZyxelCom trialService <service>`	Activates the trial services to myZyXEL.com. *service*: *1*: Content Filtering (CF) *2*: Anti-Spam (AS) + Intrusion Detection Protection (IDP) + Anti-Virus (AV) *3*: CF + AS + IDP + AV	R
`sys myZyxelCom serviceUpgrade <licence key>`	Registers a license key to myZyXEL.com.	R
`sys myZyxelCom serviceRefresh`	Gets up-to-date service status from the myZyXEL.com database.	R
`sys myZyxelCom display`	Displays the ZyWALL’s registration information.	R
`sys myZyxelCom serviceDisplay`	Displays the service status (including the expiration date if the service is already activated).	R

18.2 Country Codes

The following section lists the relationship between countries and country codes defined in the ZyWALL.

Table 64 Country Codes

COUNTRY NAME	COUNTRY CODE
AFGHANISTAN	1
ALBANIA	2
ALGERIA	3
AMERICA	4
ANDORRA	5
ANGOLA	6
ANGUILLA	7
ANTARTICA	8
ANTIGUA_AND_BARBUDA	9
ARGENTINA	10
ARMENIA	11
ARUBA	12
ASCENSION_ISLAND	13
AUSTRALIA	14
AUSTRIA	15
AZERBAIJAN	16
BAHAMAS	17
BAHRAIN	18
BANGLADESH	19
BARBADOS	20
BELARUS	21
BELGIUM	22
BELIZE	23
BENIN	24
BERMUDA	25
BHUTAN	26
BOLIVIA	27
BOSNIA_AND_HERZEGOVINA	28
BOTSWANA	29
BOUVET_ISLAND	30
BRAZIL	31
BRITISH_INDIAN_OCEAN_TERRITORY	32
BRUNEI_DARUSSALAM	33
BULGARIA	34
BURKINA_FASO	35

Table 64 Country Codes

COUNTRY NAME	COUNTRY CODE
BURUNDI	36
CAMBODIA	37
CAMEROON	38
CANADA	39
CAPE_VERDE	40
CAYMAN_ISLANDS	41
CENTRAL_AFRICAN_REPUBLIC	42
CHAD	43
CHILE	44
CHINA	45
CHRISTMAS_ISLAND	46
COCOS_KEELING_ISLANDS	47
COLOMBIA	48
COMOROS	49
CONGO_DEMOCRATIC_REPUBLIC_OF_THE	50
CONGO_REPUB_IC_OF	51
COOK_ISLANDS	52
COSTA_RICA	53
COTE_D	54
CROATIA_HRVATSKA	55
CYPRUS	56
CZECH_REPUBLIC	57
DENMARK	58
DJIBOUTI	59
DOMINICA	60
DOMINICAN_REPUBLIC	61
EAST_TIMOR	62
ECUADOR	63
EGYPT	64
EL_SALVADOR	65
EQUATORIAL_GUINEA	66
ERITREA	67
ESTONIA	68
ETHIOPIA	69
FALKLAND_ISLANDS_MALVINA	70
FAROE_ISLANDS	71
FIJI	72
FINLAND	73

Table 64 Country Codes

COUNTRY NAME	COUNTRY CODE
FRANCE	74
FRANCE_METROPOLITAN	75
FRENCH_GUIANA	76
FRENCH_POLYNESIA	77
FRENCH_SOUTHERN_TERRITORIES	78
GABON	79
GAMBIA	80
GEORGIA	81
GERMANY	82
GHANA	83
GIBRALTAR	84
GREAT_BRITAIN	85
GREECE	86
GREENLAND	87
GRENADA	88
GUADELOUPE	89
GUAM	90
GUATEMALA	91
GUERNSEY	92
GUINEA	93
GUINEA_BISSAU	94
GUYANA	95
HAITI	96
HEARD_AND_MCDONALD_ISLANDS	97
HOLY_SEE_CITY_VATICAN_STATE	98
HONDURAS	99
HONG_KONG	100
HUNGARY	101
ICELAND	102
INDIA	103
INDONESIA	104
IRELAND	105
ISLE_OF_MAN	106
ITALY	107
JAMAICA	108
JAPAN	109
JERSEY	110
JORDAN	111

Table 64 Country Codes

COUNTRY NAME	COUNTRY CODE
KAZAKHSTAN	112
KENYA	113
KIRIBATI	114
KOREA_REPUBLIC_OF	115
KUWAIT	116
KYRGYZSTAN	117
LAO_PEOPLE’s_DEMOCRATIC_REPUBLIC_OF	118
LATVIA	119
LEBANON	120
LESOTHO	121
LIBERIA	122
LIECHTENSTEIN	123
LITHUANIA	124
LUXEMBOURG	125
MACAU	126
MACEDONIA_FORMER_YUGOSLAV_REPUBLIC	127
MADAGASCAR	128
MALAWI	129
MALAYSIA	130
MALDIVES	131
MALI	132
MALTA	133
MARSHALL_ISLANDS	134
MARTINIQUE	135
MAURITANIA	136
MAURITIUS	137
MAYOTTE	138
MEXICO	139
MICRONESIA_FEDERAL_STATE_OF	140
MOLDOVA_REPUBLIC_OF	141
MONACO	142
MONGOLIA	143
MONTSERRAT	144
MOROCCO	145
MOZAMBIQUE	146
NAMIBIA	147
NAURU	148
NEPAL	149

Table 64 Country Codes

COUNTRY NAME	COUNTRY CODE
NETHERLANDS	150
NETHERLANDS_ANTILLES	151
NEW_CALEDONIA	152
NEW_ZEALAND	153
NICARAGUA	154
NIGER	155
NIGERIA	156
NIUE	157
NORFOLK_ISLAND	158
NORTHERN_MARIANA_ISLANDS	159
NORWAY	160
NOT_DETERMINED	161
OMAN	162
PAKISTAN	163
PALAU	164
PANAMA	164
PAPUA_NEW_GUINEA	166
PARAGUAY	167
PERU	168
PHILIPPINES	169
PITCAIRN_ISLAND	170
POLAND	171
PORTUGAL	172
PUERTO_RICO	173
QATAR	174
REUNION_ISLAND	175
ROMANIA	176
RUSSIAN_FEDERATION	177
RWANDA	178
SAINT_KITTS_AND_NEVIS	179
SAINT_LUCIA	180
SAINT_VINCENT_AND_THE_GRENADINES	181
SAN_MARINO	182
SAO_TOME_AND_PRINCIPE	183
SAUDI_ARABIA	184
SENEGAL	185
SEYCHELLES	186
SIERRA_LEONE	187

Table 64 Country Codes

COUNTRY NAME	COUNTRY CODE
SINGAPORE	188
SLOVAK_REPUBLIC	189
SLOVENIA	190
SOLOMON_ISLANDS	191
SOMALIA	192
SOUTH_AFRICA	193
SOUTH_GEORGIA_AND_THE_SOUTH_SANDWICH_ISLANDS	194
SPAIN	195
SRI_LANKA	196
ST_PIERRE_AND_MIQUELON	197
ST_HELENA	198
SURINAME	199
SVALBARD_AND_JAN_MAYEN_ISLANDS	200
SWAZILAND	201
SWEDEN	202
SWITZERLAND	203
TAIWAN	204
TAJIKISTAN	205
TANZANIA	206
THAILAND	207
TOGO	208
TOKELAU	209
TONGA	210
TRINIDAD_AND_TOBAGO	211
TUNISIA	212
TURKEY	213
TURKMENISTAN	214
TURKS_AND_CAICOS_ISLANDS	215
TUVALU	216
US_MINOR_OUTLYING_ISLANDS	217
UGANDA	218
UKRAINE	219
UNITED_ARAB_EMIRATES	220
UNITED_KINGDOM	221
UNITED_STATES	222
URUGUAY	223
UZBEKISTAN	224
VANUATU	225

Table 64 Country Codes

COUNTRY NAME	COUNTRY CODE
VENEZUELA	226
VIETNAM	227
VIRGIN_ISLANDS_BRITISH	228
VIRGIN_ISLANDS_USA	229
WALLIS_AND_FUTUNA_ISLANDS	230
WESTERN_SAHARA	231
WESTERN_SAMOA	232
YEMEN	233
YUGOSLAVIA	234
ZAMBIA	235
ZIMBABWE	236

18.3 Command Examples

This example displays your ZyWALL’s registration information. .

```
ras> sys myZyxelCom display

register server address : www.myzyxel.com
register server path : /register/registration?

username : aseawfasf
password : aaaaaa

email : aa@aa.aa.aa

sku : CFRT=1&CFST=319&ZASS=469&ISUS=469&ZAVS=469

country code : 204

register state 1

register MAC : 0000AA220765
CF expired day : 2008-05-26 14:58:19
AS expired day : 2008-10-23 14:58:19
2In1 expired day : 2008-10-23 14:58:19
Last update day : 2007-07-12 14:58:19
```

Table 65 sys myZyxelCom display Command Output

FIELD NAME	DESCRIPTION
register server address	Displays the URL of the registration server.
register server path	Displays the path storing your ZyWALL’s registration information on the registration server.
username	Displays the registered username.

Table 65 sys myZyxelCom display Command Output

FIELD NAME	DESCRIPTION
password	Displays the registered password.
email	Displays the registered e-mail address.
sku	This is a string the registration server uses to validate your ZyWALL.
country code	Displays the registered country code.
register state	Displays whether the ZyWALL has completed the product registration. 1: Yes 0: No
register MAC	Displays the MAC address of the ZyWALL. This is also the unique MAC address used for product registration on the registration server.
CF expired day	Displays the due date that you can use the Content Filter service on this ZyWALL.
AS expired day	Displays the due date that you can use the Anti Spam service on this ZyWALL.
2In1 expired day	Displays the due date that you can use the Anti Virus and IDP services on this ZyWALL.
Last update day	Displays the most recent date that you updated the signatures for all services including CF, AS, AV, and IDP.

This example displays the detailed service registration information of your ZyWALL.

```
ras> sys myZyxelCom serviceDisplay
Content Filter Service :
Actived, Licenced, Trial, Expired : 2007-07-08 16:36:15
Anti-Spam Service :
Actived, Licenced, Trial, Expired : 2007-09-06 16:36:18
IDP/Anti-Virus Service :
Actived, Licenced, Trial, Expired : 2007-09-06 16:36:18
ras>
```

Table 66 sys myZyxelCom serviceDisplay Command Output

FIELD NAME	DESCRIPTION
Content Filter Service Anti-Spam Service IDP/Anti-Virus Service	This is the service name.
Actived Non-actived	Displays if the service is enabled or not. If the server has not activated yet, it just displays `non-actived` without further information as following fields.
Licenced Expired	Displays the service status.
Trial Standard	Displays the service license type.
Expired : date	Displays the expiration date of the service.

19

PPPoE Commands

Use these commands to configure PPPoE settings on the ZyWALL.

19.1 Command Summary

A remote node is the remote gateway (and the network behind the remote gateway) across a WAN connection. Remote node 1 may be your ISP for example. You may configure multiple remote nodes in products with SMT menus or those with multiple WAN ports. In products without SMT menus or multiple WAN ports, a remote node is the ISP you configured in the web configurator.

A channel is a subset of an interface, such as a LAN or WAN interface. An interface may have more than one channel, but it usually has just one. The *channel-name* is the encapsulation method used for the WAN dial-up WAN link.

The following section lists the commands for this feature.

Table 67 poe Command Summary

COMMAND	DESCRIPTION	M
`poe channel disable <CHANNEL>`	Disables a PPPoE channel.	H+R
`poe channel enable <CHANNEL>`	Enables a channel to carry PPPoE traffic.	H+R
`poe channel show`	Shows the PPPoE channels available.	H+R
`poe debug [ON|OFF]`	Switches the PPPoE debug function on or off.	H+R
`poe status`	Shows the status of the ZyWALL PPoE channels.	R
`poe status [`*`channel-name`*`]`	Displays the status of packets on a specified PPoE channel. *`channel-name:`* Channel names are “poe0” or “poe1”.	R
`poe drop <`*`channel`*`>`	Drops a PPPoE link to the specified channel, for example, “poe0”.	R
`poe dial <`*`node`*`>`	Dials a link to the specified remote node, for example “WAN_1”.	R
`poe ether [rfc|3com]`	Sets or displays the EtherType. The EtherType indicates which protocol a packet uses. You can set the EtherType so that either RFC or 3Com protocols are used.	R
`poe inout <NODE_NAME>`	Sets the call direction between ZyWALL and a node to both.	H+R
`poe ippool [IP] [CNT]`	Sets or displays PPPoE IP pool information.	H+R
`poe master easy [ON|OFF]`	Switches the response for a no service name request on or off.	H+R
`poe master promiscuous [ON|OFF]`	Provides a PPPoE server list to clients	H+R

Table 67 poe Command Summary (continued)

COMMAND	DESCRIPTION	M
`poe padt [LIMIT]`	Sets/displays the PPPoE PADT limit.	H+R
`poe proxy active [ON|OFF]`	Turns the PPPoE proxy function on / off. Note: proxy commands will be removed.	R
`poe proxy debug [ON|OFF]`	Turns the PPPoE proxy debug function on / off.	R
`poe proxy disp`	Displays the PPPoE proxy client session table.	R
`poe proxy flush`	Clears the PPPoE proxy client session table.	R
`poe proxy init`	Initializes the PPPoE proxy client session table.	R
`poe proxy time [INTERVAL]`	Sets the time out interval, it’s a count. Actual time is count * 5 seconds.	R
`poe retry count [COUNT]`	Sets/displays the PPPoE retry count.	H+R
`poe retry interval [INTERVAL]`	Sets/displays the PPPoE retry interval.	H+R
`poe service add <SERVICE-NAME>`	Adds a PPPoE service.	H+R
`poe service show`	Shows a PPPoE service.	H+R

The following table shows a list of default values.

Table 68 poe Default Values

VARIABLE	DEFAULT VALUE
`EtherType [rfc|3com]`	rfc

19.2 Command Examples

This example shows the status of channel poe0. Specifically it will show how many incoming and outgoing packets, octets (bytes) and control packets (packets used to set up or tear down the link) there are.

```
ras> poe status poe0
chann 'poe0'
state 0, bad pkt= 0
I/C pkt= 0          octet= 0         , ctrl pkt= 0
O/G pkt= 0          octet= 0         , ctrl pkt= 0
```

This example shows dialing up remote node *wan_1* using PPPoE.

```
ras> poe dial WAN_1
Start dialing for node <WAN_1>...
### Hit any key to continue.###
$$$ DIALING dev=6 ch=0..........
$$$ OUTGOING-CALL phone()
$$$ CALL CONNECT speed<100000000> type<6> chan<0>
$$$ LCP opened
$$$ PAP sending user/pswd
$$$ IPCP negotiation started
$$$ IPCP neg' Primary DNS 192.168.30.1
$$$ IPCP neg' Primary DNS 172.23.5.2
$$$ IPCP opened
```

20

PPTP Commands

Use these commands to configure PPTP settings on the ZyWALL.

20.1 Command Summary

A remote node is the remote gateway (and the network behind the remote gateway) across a WAN connection. Remote node 1 may be your ISP for example. You may configure multiple remote nodes in products with SMT menus or those with multiple WAN ports. In products without SMT menus or multiple WAN ports, a remote node is the ISP you configured in the web configurator.

The following section lists the commands for this feature.

Table 69 pptp Command Summary

COMMAND	DESCRIPTION	M
`pptp debug [ON|OFF]`	Activates/deactivates the PPTP debug flag.	H+ R
`pptp dial <`*`remote-node-name`*`>`	Initiates a PPTP tunnel to the specified remote node.	R
`pptp drop <`*`remote-node-name`*`>`	Drops a PPTP tunnel to the specified remote node.	R
`pptp tunnel <`*`tunnel-id`*`>`	Displays the status of the specified PPTP tunnel. The status is either active or not active. *`tunnel-id:`* Options are 1 or 2.	R
`pptp enque [`*`size`*`]`	This command is used for flow control. It limits the number of packets queued for transmission to the number you enter here. Extra packets are dropped. *`size`*`:` Enter a number between 1 and 2147483647.	R
`pptp chapv1LM [on|off]`	Activates or deactivates MS CHAP v1 LAN Manager Authentication. This procedure authenticates a user when connecting to an ISP.	R

The following table shows a list of default values.

Table 70 pptp Default Values

VARIABLE	DEFAULT VALUE
`chapv1LM [on|off]`	off
`enque size`	10

20.2 Command Examples

This example limits the number of packets queued for transmission to 11. Packets 12 and above in the queue will be dropped.

```
ras> pptp enque 11
PPTP max en-queue size (flow control) = 11
```

21

System Commands

Use these commands to configure system related settings on the ZyWALL.

21.1 Local User Database Commands

The following section lists the local user database commands.

Table 71 Local User Database Commands

COMMAND	DESCRIPTION	M
sys authserver localuser disp <all|*index*>	Displays the local user database.	R+B
sys authserver localuser edit <*index*> <0:inactive|1:active> <*username*> <*password*>	Edits the local user database.	R+B
sys authserver localuser load	Loads local user database information.	R+B
sys authserver localuser save	Saves the local user database.	R+B

21.2 Local User Database Commands Example

The following example configures a local user account with username example and password test.

```
ras> sys authserver localuser load
ras> sys authserver localuser edit 1 1 example test
ras> sys authserver localuser save
```

21.3 Date and Time Commands

The following section lists the date and time commands.

Table 72 Date and Time Commands

COMMAND	DESCRIPTION	M
sys datetime date [*yyyy mm dd*]	Sets or displays the system's current date (in year month day format).	R+B
sys datetime period [*day*]	Sets or displays the time period (in days) for how often the ZyWALL synchronizes with the time server.	R+B

Table 72 Date and Time Commands (continued)

COMMAND	DESCRIPTION	M
sys datetime sync	Has the ZyWALL synchronize with the time server.	R+B
sys datetime time *hh* [*mm* [*ss*]]	Sets or displays the system's current time (in hour minute second format).	R+B

21.4 Diagnostic Commands

The following section lists the diagnostic commands.

Table 73 Diagnostic Commands

COMMAND	DESCRIPTION	M
sys diagnostic console	Sends the diagnostic file through the console port.	R+B
sys diagnostic load	Use this command to be able to use other commands to configure the ZyWALL's diagnostic settings.	R+B
sys diagnostic mail authEnable [on|off]	Enables or disables SMTP (Simple Mail Transfer Protocol) SMTP authentication.	R+B
sys diagnostic mail authPassword <*password*>	Sets the SMTP authentication password.	R+B
sys diagnostic mail authUser <*username*>	Specifies (or displays) the user name (up to 31 characters) for the e-mail account the ZyWALL uses for e-mailing diagnostic files.	R+B
sys diagnostic mail mailDisplay	Shows the currently saved diagnostic e-mail settings.	R+B
sys diagnostic mail mailReceiver <*ip-address|domain-name*>	Specifies (or displays) the e-mail address to which the ZyWALL sends the diagnostic files.	R+B
sys diagnostic mail mailSender <*ip-address|domain-name*>	Specifies (or displays) the address in the from/sender line of the diagnostic e-mail message that the ZyWALL sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server.	R+B
sys diagnostic mail mailServer <*ip-address|domain-name*>	Specifies (or displays) the server name or the IP address of the mail server for the e-mail address specified as the mail sender.	R+B
sys diagnostic mail mailSubject <*email-subject*>	Specifies the title in the subject line of the diagnostic e-mail message that the ZyWALL sends.	R+B
sys diagnostic mail send	Generates and sends a diagnostic e-mail.	R+B
sys diagnostic save	Saves the diagnostic settings you configured to non-volatile memory.	R+B
sys diagnostic schedule display	Shows the current schedule for sending diagnostic files.	R+B
sys diagnostic schedule hour <0~23>	Sets the hour for sending diagnostic files.	R+B
sys diagnostic schedule minute <0~59>	Sets the minute for sending diagnostic files.	R+B
sys diagnostic schedule policy <0:hourly|1:daily|2:weekly|3:none>	Sets how often the ZyWALL sends periodic diagnostic files.	R+B

Table 73 Diagnostic Commands (continued)

COMMAND	DESCRIPTION	M
`sys diagnostic switch [on|off]`	Turns the diagnostic feature on or off.	R+B
`sys diagnostic threshold CPU [0~100]`	Sets the ZyWALL to generate and send a diagnostic file every time the CPU usage exceeds the specified percent for more than 60 seconds. 0 disables generation and sending of diagnostic files based on CPU usage.	R+B

21.4.1 Logs Commands

The following section lists the logs commands.

Table 74 Logs Commands

COMMAND	DESCRIPTION	M
`sys logs category 8021x [0:none|1:log] [0:don't show debug type|1:show debug type]`	Records logs for IEEE 802.1X.	R+B
`sys logs category access [0:none|1:log|2:alert|3:both] [0:don't show debug type|1:show debug type]`	Records access control logs and/or sends alerts.	R+B
`sys logs category as [0:none|1:log]`	Records anti-spam logs and/or sends alerts.	R+B
`sys logs category attack [0:none|1:log|2:alert|3:both] [0:don't show debug type|1:show debug type]`	Records firewall attack logs and/or sends alerts.	R+B
`sys logs category av [0:none|1:log|2:alert|3:both] [0:don't show debug type|1:show debug type]`	Records anti-virus logs and/or sends alerts.	R+B
`sys logs category cdr [0:none|1:log] [0:don't show debug type|1:show debug type]`	Records Call Detail Record logs.	R+B
`sys logs category display`	Displays the log settings for the categories of logs.	R+B
`sys logs category error [0:none|1:log|2:alert|3:both] [0:don't show debug type|1:show debug type]`	Records system error logs and/or sends alerts.	R+B
`sys logs category icmp [0:none|1:log]`	Records ICMP logs.	R+B
`sys logs category idp [0:none|1:log|2:alert|3:both] [0:don't show debug type|1:show debug type]`	Records IDP logs and/or sends alerts.	R+B
`sys logs category ike [0:none|1:log|2:alert|3:both] [0:don't show debug type|1:show debug type]`	Records IKE logs and/or sends alerts.	R

Table 74 Logs Commands (continued)

COMMAND	DESCRIPTION	M
`sys logs category ipsec [0:none|1:log|2:alert|3:both] [0:don't show debug type|1:show debug type]`	Records IPSec logs and/or sends alerts.	R
`sys logs category javablocked [0:none|1:log|2:alert|3:both] [0:don't show debug type|1:show debug type]`	Records blocked web feature logs and/or sends alerts.	R+B
`sys logs category mten [0:none|1:log] [0:don't show debug type|1:show debug type]`	Records system maintenance logs.	R+B
`sys logs category packetfilter [0:none|1:log] [0:don't show debug type|1:show debug type]`	Records packet filter logs.	R+B
`sys logs category pki [0:none|1:log|2:alert|3:both] [0:don't show debug type|1:show debug type]`	Records certificate logs.	R+B
`sys logs category ppp [0:none|1:log] [0:don't show debug type|1:show debug type]`	Records PPP logs.	R
`sys logs category remote [0:none|1:log] [0:don't show debug type|1:show debug type]`	Records remote management logs.	R+B
`sys logs category tcpreset [0:none|1:log] [0:don't show debug type|1:show debug type]`	Records TCP reset logs.	R+B
`sys logs category tls [0:none|1:log|2:alert|3:both] [0:don't show debug type|1:show debug type]`	Records TLS (HTTPS) logs.	R+B
`sys logs category traffic [0:none|1:log] [0:don't show debug type|1:show debug type]`	Records traffic logs.	R+B
`sys logs category upnp [0:none|1:log] [0:don't show debug type|1:show debug type]`	Records UPnP logs.	R
`sys logs category urlblocked [0:none|1:log|2:alert|3:both] [0:don't show debug type|1:show debug type]`	Records blocked web access logs and/or sends alerts.	R+B
`sys logs category urlforward [0:none|1:log] [0:don't show debug type|1:show debug type]`	Records forwarded web access logs and/or sends alerts.	R+B
`sys logs category wireless [0:none|1:log] [0:don't show debug type|1:show debug type]`	Records wireless logs.	R+B
`sys logs clear`	Clears all logs.	R+B
`sys logs consolidate msglist`	Displays the consolidated messages.	R+B

Table 74 Logs Commands (continued)

COMMAND	DESCRIPTION	M
`sys logs consolidate period <1-600>`	Sets the log consolidation period (seconds).	R+B
`sys logs consolidate switch <0:on|1:off>`	Enables or disables log consolidation.	R+B
`sys logs display [access|attack|error|ipsec|ike|javablocked|mten|packetfilter|pki|tcpreset|urlblocked|urlforward]`	Displays all logs or specific categories of logs.	R+B
`sys logs errlog clear`	Clears error logs.	R+B
`sys logs errlog disp`	Displays error logs.	R+B
`sys logs errlog online`	Turns the error log online display on or off.	R+B
`sys logs lastAlert <`*`index`*`>`	Displays the last #index alert in the centralized log.	R+B
`sys logs load`	Loads the log settings for editing. Use this command before you configure the log settings. Use `sys logs save` after you configure the log settings.	R+B
`sys logs mail alertAddr [`*`mail-address`*`]`	Sets the e-mail address to which the ZyWALL sends alerts.	R+B
`sys logs mail auth <0:enable|1:disable>`	Enables or disables SMTP (Simple Mail Transfer Protocol) SMTP authentication.	R+B
`sys logs mail clearLog [0:no|1:yes]`	Sets whether or not the ZyWALL clears the log after sending logs by e-mail.	R+B
`sys logs mail display`	Displays the settings for e-mailing logs.	R+B
`sys logs mail logAddr [`*`mail-address`*`]`	Sets or displays the e-mail address to send logs to.	R+B
`sys logs mail passwd [`*`smtp-user-password`*`]`	Sets the SMTP authentication password.	R+B
`sys logs mail port [`*`port`*`]`	Sets the port number for sending log e-mails.	R+B
`sys logs mail schedule display`	Displays the log e-mail schedule.	R+B
`sys logs mail schedule hour <0-23>`	Sets the hour to send the logs.	R+B
`sys logs mail schedule minute <0-59>`	Sets the minute to send the logs.	R+B
`sys logs mail schedule policy <0:full|1:hourly|2:daily|3:weekly|4:none>`	Sets how often the ZyWALL sends log e-mails.	R+B
`sys logs mail schedule week <0:sun|1:mon|2:tue|3:wed|4:thu|5:fri|6:sat>`	Sets the day of the week to send the e-mail log.	R+B
`sys logs mail senderAddr <`*`mail-address`*`>`	Specifies the e-mail address in the from/sender line of the log e-mail message that the ZyWALL sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server.	R+B
`sys logs mail server <`*`domain-name|ip`*`>`	Specifies the server name or the IP address of the mail server for the e-mail address specified as the mail sender.	R+B
`sys logs mail subject <`*`mail-subject`*`>`	Specifies the title in the subject line of the diagnostic e-mail message that the ZyWALL sends.	R+B

Table 74 Logs Commands (continued)

COMMAND	DESCRIPTION	M
`sys logs mail user [`*`smtp-username`*`]`	Specifies (or displays) the user name (up to 31 characters) for the e-mail account the ZyWALL uses for e-mailing logs.	R+B
`sys logs save`	Saves the log settings to non-volatile memory.	R+B
`sys logs switch asmlog <0:no|1:yes>`	Enables or disables asymmetrical route logs.	R+B
`sys logs switch bmlog <0:no|1:yes>`	Enables or disables broadcast and multicast logs.	R+B
`sys logs switch display`	Displays the switch log settings.	R+B
`sys logs switch dynacllog <0:no|1:yes>`	Enables or disables dynamic firewall logs.	R+B
`sys logs syslog active [0:no|1:yes]`	Enables or disables the UNIX syslog.	R+B
`sys logs syslog display`	Displays the syslog settings.	R+B
`sys logs syslog facility <1-7>`	Logs the messages to different files.	R+B
`sys logs syslog server [`*`domain name`*`|`*`ip-address`*`]`	This sets the domain name and IP address for the syslog server to send the logs.	R+B
`sys logs updateSvrIP <`*`minute`*`>`	Sets how often to resolve the mail and syslog server domain name to an IP address.	R+B

21.5 Configuring What You Want the ZyWALL to Log

1. Use the `sys logs load` command to load the log settings for editing. Then you can configure which logs the ZyWALL is to record.
2. Use `sys logs category` to view a list of the log categories.

Figure 8 Displaying Log Categories Example

```
ras> sys logs category
8021x           access          attack          display
error           icmp            ike             ipsec
javablocked     mten            packetfilter    ppp
cdr             pki             tls             remote
tcpreset        traffic         upnp            urlblocked
urlforward      wireless
```

3. Use `sys logs category` followed by a log category to display the parameters that are available for the category.

Figure 9 Displaying Log Parameters Example

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both] [0:don't show debug type/1:show debug
type]
```

4. Use `sys logs category` followed by a log category and a parameter to decide what to record.

   Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.
5. Use the `sys logs save` command to store the settings in the ZyWALL (you must do this in order to record logs).

21.5.1 Displaying Logs

- Use the `sys logs display` command to show all of the logs in the ZyWALL's log.
- Use the `sys logs category display` command to show the log settings for all of the log categories.
- Use the `sys logs display [log category]` command to show the logs in an individual ZyWALL log category.
- Use the `sys logs clear` command to erase all of the ZyWALL's logs.

21.5.2 Log Command Example

This example shows how to set the ZyWALL to record the access logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access

#  .time                 source                 destination            notes

    message
  0|06/08/2004 05:58:21 |172.21.4.154         |224.0.1.24           |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  1|06/08/2004 05:58:20 |172.21.3.56          |239.255.255.250      |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  2|06/08/2004 05:58:20 |172.21.0.2           |239.255.255.254      |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  3|06/08/2004 05:58:20 |172.21.3.191         |224.0.1.22           |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  4|06/08/2004 05:58:20 |172.21.0.254         |224.0.0.1            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  5|06/08/2004 05:58:20 |172.21.4.187:137     |172.21.255.255:137   |ACCESS
BLOCK
    Firewall default policy: UDP (W to W/ZW)
```

21.6 Remote Node Commands

The following section lists the remote node commands.

Table 75 Remote Node Commands

COMMAND	DESCRIPTION	M
`sys rn accessblock <0:disable|1:enable>`	Blocks or allows access to the remote node.	R
`sys rn disp <entry#>`	Displays remote node information. If you have loaded a remote node entry, use 0 to display it.	R
`sys rn load <entry#>`	Loads remote node information.	R
`sys rn mtu <576~1500>`	Sets the Maximum Transmission Unit number of bytes for the remote node entry.	R
`sys rn nailup <no|yes>`	Configures the remote node's nailed up setting.	R
`sys rn nat <none|sua|full_feature>`	Configures the NAT type for the remote node entry.	R
`sys rn pingDrop <1:WAN1|2:WAN2> <on|off>`	Drop the connection if the ping check fails.	R
`sys rn save [index]`	Saves remote node's settings.	R
`sys rn trigger <on|off>`	Enables or disables trigger dial for the remote node.	R

21.7 Remote Management Commands

The following section lists the server (remote management) commands.

Table 76 Remote Management Commands

COMMAND	DESCRIPTION	M
`sys server access <telnet|ftp|ssh|http|https|icmp|snmp|dns><lan|wan1|wan2|dmz|wlan><on|off>`	Enables or disables the access type on the specified interface.	R+B
`sys server auth_client <https> [on|off]`	Specifies whether the ZyWALL authenticates the client for the specified service's sessions.	R+B
`sys server certificate <https|ssh> [certificate-name]`	Sets the server certificate the ZyWALL uses to identify itself for the specified service's sessions.	R+B
`sys server disp`	Display's the ZyWALL's server access settings.	R+B
`sys server load`	Loads server information. Use this to be able to configure the server settings.	R+B
`sys server port <telnet|ftp|ssh|http|https|snmp> <port>`	Sets the server port number.	R+B
`sys server save`	Saves the server settings.	R+B
`sys server secureip <telnet|ftp|ssh|http|https|icmp|snmp|dns> <ip>`	Sets the IP address of a "trusted" computer that is allowed to communicate with the ZyWALL using this service.	R+B

21.8 Remote Management Commands Example

The following example allows HTTPS management access to the ZyWALL through WAN1 from IP address 2.2.2.2 and displays the server access settings.

```
ras> sys server load
ras> sys server access https wan1 on
ras> sys server secureip https 2.2.2.2
ras> sys server save
ras> sys server disp

 TELNET server
  Server Port=    23, Access= LAN+WAN1+DMZ+WLAN+WAN2, Secure Ip= 0.0.0.0

 FTP server
  Server Port=    21, Access= LAN+WAN1+DMZ+WLAN+WAN2, Secure Ip= 0.0.0.0

 SSH server
       Certificate = auto_generated_self_signed_cert
  Server Port=    22, Access= LAN+WAN1+DMZ+WLAN+WAN2, Secure Ip= 0.0.0.0

 HTTPS server
       Certificate = auto_generated_self_signed_cert
       Authenticate Client Certificates = No
  Server Port=   443, Access= LAN+WAN1+DMZ+WLAN+WAN2, Secure Ip= 2.2.2.2

 HTTP server
  Server Port=    80, Access= LAN+WAN1+DMZ+WLAN+WAN2, Secure Ip= 0.0.0.0

 ICMP ping
                      Access= LAN+WAN1+DMZ+WLAN+WAN2, Secure Ip= 0.0.0.0

 SNMP service
  Server Port=   161, Access= LAN+WAN1+DMZ+WLAN+WAN2, Secure Ip= 0.0.0.0

 DNS service
  Server Port=    53, Access= LAN+WAN1+DMZ+WLAN+WAN2, Secure Ip= 0.0.0.0
```

21.9 Threat Report Commands

The following section lists the threat report commands.

Table 77 Threat Report Commands

COMMAND	DESCRIPTION	M
`sys threatReport as <id:IDP-ID|src:source IP|dst:destination IP>`	Displays the top anti-spam statistic records by virus name, source IP address, or destination IP address.	R+B
`sys threatReport as active`	Turns anti-spam threat reports on or off.	R+B
`sys threatReport as flush`	Discards all anti-spam report data and updates the time stamp.	R+B
`sys threatReport as summary`	Displays a summary of the anti-spam statistics.	R+B

Table 77 Threat Report Commands (continued)

COMMAND	DESCRIPTION	M
`sys threatReport av active <yes|no>`	Turns anti-virus threat reports on or off.	R+B
`sys threatReport av flush`	Discards all anti-virus report data and updates the time stamp.	R+B
`sys threatReport av statistic <id:AV-ID|src:source IP|dst:destination IP>`	Displays the top anti-virus statistic records by virus name, source IP address, or destination IP address.	R+B
`sys threatReport av summary`	Displays a summary of the anti-virus statistics.	R+B
`sys threatReport debug <yes:no>`	Turns the threat reports debug flag on or off.	R+B
`sys threatReport idp active <yes|no>`	Turns IDP threat reports on or off.	R+B
`sys threatReport idp flush`	Discards all IDP report data and updates the time stamp.	R+B
`sys threatReport idp statistic <id:IDP-ID|src:source IP|dst:destination IP>`	Displays the top IDP statistic records by signature ID, source IP address, or destination IP address.	R+B
`sys threatReport idp summary`	Displays a summary of the IDP statistics.	R+B

21.10 Temporarily Open Session Commands

The following section lists the Temporarily Open Session (TOS) commands.

Table 78 TOS Commands

COMMAND	DESCRIPTION	M
`sys tos allow_FinPshAck <on|off>`	Turn this on to allow packets with a FIN, PSH, or ACK flag.	R+B
`sys tos debug <on|off>`	Turns TOS debug message on or off.	R+B
`sys tos display`	Shows all runtime Temporarily Open Sessions.	R+B
`sys tos fwSchedule active [on|off]`	Applies the firewall schedule policy to existing sessions.	R+B
`sys tos fwSchedule debug [on|off]`	Turns fwSchedule debug messages on or off.	R+B
`sys tos listPerHost`	Displays the session count for each host.	R+B
`sys tos sessPerHost <1~10000>`	Sets the temporary open sessions per host limit.	R+B
`sys tos tempTOSDisplay`	Displays the temporal TOS records.	R+B
`sys tos tempTOSTimeout [1~2147483647]`	Sets or displays the temporal timeout value in seconds.	R+B
`sys tos timeout ah <1~65535>`	Sets the AH-session idle-timeout value (used in IPsec) in seconds.	R+B
`sys tos timeout display`	Displays all TOS (Temporarily Open Session) timeout information.	R+B
`sys tos timeout esp <1~65535>`	Sets the ESP-session idle-timeout value (used in IPsec) in seconds.	R+B
`sys tos timeout gre <1~65535>`	Sets the GRE-session idle-timeout value in seconds.	R+B
`sys tos timeout icmp <1~65535>`	Sets the ICMP session idle timeout value in seconds.	R+B
`sys tos timeout igmp <1~65535>`	Sets the IGMP session idle timeout value in seconds.	R+B

Table 78 TOS Commands (continued)

COMMAND	DESCRIPTION	M
`sys tos timeout mail <1~65535>`	Sets the e-mail session idle-timeout value in seconds.	R+B
`sys tos timeout others <1~65535>`	Sets the idle-timeout value for other sessions in seconds.	R+B
`sys tos timeout tcp <1~65535>`	Sets the TCP session idle timeout value in seconds.	R+B
`sys tos timeout tcpfin <1~65535>`	Sets the TCP FIN session idle timeout value in seconds.	R+B
`sys tos timeout tcpsyn <1~65535>`	Sets the SYN TCP session idle timeout value in seconds.	R+B
`sys tos timeout udp <1~65535>`	Sets the UDP-session idle-timeout value in seconds.	R+B

21.10.1 UPnP Commands

The following section lists the UPnP commands.

Table 79 UPnP Commands

COMMAND	DESCRIPTION	M
`sys upnp active [0:no/1:yes]`	Turns UPnP on or off.	R
`sys upnp config [0:no/1:yes]`	Allow UPnP to configure NAT rules or not.	R
`sys upnp debug [on|off]`	Turns UPnP debug message on or off.	R
`sys upnp display`	Displays the UPnP configuration.	R
`sys upnp firewall [0:deny|1:pass]`	Allow UPnP to pass through the firewall.	R
`sys upnp load`	Loads the UPnP settings for editing. Use this command to be able to configure the settings. Use `sys upnp save` after you configure the settings.	R
`sys upnp reserve [0:deny|1:permit]`	Retain UPnP created NAT rules even after restarting.	R
`sys upnp save`	Saves the UPnP settings to the non-volatile memory.	R

21.10.2 UPnP Commands Example

The following example turns on UPnP and sets the ZyWALL to allow UPnP to create firewall rules and keep UPnP created NAT rules even after restarting.

```
ras> sys upnp load
ras> sys upnp active 1
ras> sys upnp config 1
ras> sys upnp reserve 1
ras> sys upnp save
ras> sys upnp display

                              Active:  Yes
     Reserve UPnP NAT rules in flash:  Yes
          Configuration through UPnP:  Permit
               Pass through Firewall:  Deny
```

21.10.3 Other System Commands

The following section lists miscellaneous system commands.

Table 80 Other sys Commands

COMMAND	DESCRIPTION	M
`sys atsh`	Displays system information.	R+B
`sys baud <1~5>`	Sets the console port speed. 1: 38400 bps, 2: 19200 bps, 3: 9600, 4: 57600, 5: 115200.	R+B
`sys callhist display`	Displays the call history.	R
`sys callhist remove <index>`	Removes an entry from the call history.	R
`sys countrycode [countrycode]`	Sets or displays the country code. See Table 64 on page 136 for the country codes.	R+B
`sys cpu display`	Displays the CPU utilization.	R+B
`sys ddns debug <0:off|1:on>`	Enables or disables the DDNS debug service.	R+B
`sys ddns display <index>`	Displays DDNS information for the specified entry.	R+B
`sys ddns restart <interface>`	Updates DDNS on the specified interface.	R+B
`sys domainname [domain-name]`	Sets or displays the domain name.	R+B
`sys edit <filename>`	Edits the system preset text files such as autoexec.net.	R+B
`sys feature`	Displays information on available features.	R+B
`sys filter netbios config <0~10> <on|off>`	NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets can cause unwanted calls. Use this command to turn the NetBIOS filter on or off for the specified traffic. 0: Between LAN and WAN1 1: Between LAN and DMZ 2: Between WAN1 and DMZ 3: IPSec pass through 4: Trigger Dial 5: Between LAN and WLAN 6: Between WAN1 and WLAN 7: Between DMZ and WLAN 8: Between WAN2 and LAN 9: Between WAN2 and DMZ 10: Between WAN2 and WLAN Use on to block NetBIOS traffic flowing in the specified direction or `off` to allow it.	R+B
`sys filter netbios disp`	Displays the NetBIOS filter status.	R+B
`sys firewall`	See Chapter 13 on page 87 for details on the these commands.	R+B
`sys hostname [hostname]`	Sets or displays the system hostname.	R+B
`sys md5 <string>`	Hashes the string using MD5. The maximum length of the string is 64.	R+B
`sys mode [router|bridge|zero]`	Sets the ZyWALL to router, bridge, or zero configuration mode (zero configuration mode applies to the ZyWALL P1).	R+B
`sys myZyxelCom`	See Chapter 18 on page 135 for details on these commands.	R
`sys probeType [icmp | arp]`	Sets the DHCP server probing type.	R+B

Table 80 Other sys Commands (continued)

COMMAND	DESCRIPTION	M
`sys pwderrtm [`*`minute`*`]`	Sets or displays the password error blocking timeout value. Brute-force password guessing protection allows you to specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered.	R+B
`sys reboot`	Restarts the ZyWALL.	R+B
`sys restart daily <`*`hour`*`>`	Sets the ZyWALL to restart every day at the specified hour (24 hour format).	
`sys restart display`	Shows the ZyWALL's restart schedule.	
`sys restart timer <`*`minute`*`>`	Has the ZyWALL restart after the specified number of minutes.	
`sys roadrunner debug <0:disable|1:enable>`	Enables or disables the Roadrunner service.	R
`sys roadrunner display <`*`interface`*`>`	Displays roadrunner information for the specified interface (`enif0` or `wanif0`).	R
`sys roadrunner restart <`*`interface`*`>`	Restarts the Roadrunner service on the specified interface.	R
`sys romreset`	Restores the default romfile (configuration).	R+B
`sys socket`	Displays the system socket's ID #, type, control block address (PCB), IP address and port number of peer device connected to the socket (Remote Socket) and task control block (Owner).	R+B
`sys stdio [`*`minute`*`]`	Sets the management session inactivity timeout value.	R+B
`sys updateServer debug type <0:Disable|1:updateServer <on|off>|2:httpClient <on|off>|3:All>`	Turns the update server debug flags on or off. `0`: Disables both update server debug flags. 1: Enables or disables the update server debug flag. 2: Enables or disables the HTTP client debug flag. 3: Enables both update server debug flags.	R+B
`sys updateServer display`	Shows the address and path of the update server (for updating the anti-virus and IDP signatures).	R+B
`sys updateServer signatureUpdate`	Update the anti-virus and IDP signatures.	R+B
`sys upnp active [0:no|1:yes]`	Activates or deactivates the saved UPnP settings.	R
`sys upnp config [0:deny|1:permit]`	Allow users to make configuration changes through UPnP.	R
`sys version`	Displays the firmware and bootbase versions.	R+B
`sys view <`*`filename`*`>`	Displays the specified text file.	R+B
`sys wdog cnt [`*`value`*`]`	Sets (0~34463) or displays the current watchdog count (in 1.6 second units).	R+B
`sys wdog switch [on|off]`	Turns the watchdog firmware protection feature on or off.	R+B

22

Wireless Commands

Use these commands to configure wireless settings on the ZyWALL.

22.1 Command Summary

The following section lists the commands for this feature.

Table 81 General Wireless Commands

COMMAND	DESCRIPTION	M
`wlan active <1:on|0:off>`	Sets 1 to activate the wireless card.	R+B
`wlan association`	Displays the wireless client association list.	R+B
`wlan chid <channel-id>`	Sets the operating frequency/channel depending on your particular region. *channel-id*: This is a three-digit number. For example, *001* means the channel 1 while *010* means the channel 10.	R+B
`wlan essid <essid>`	Sets the wireless AP's SSID.	R+B
`wlan fraThreshold <256~2346>`	Sets the fragmentation threshold value.	R+B
`wlan iapp`	Displays the Inter Access Point Protocol (IAPP) information.	R+B
`wlan outputpower <0~4>`	Sets the output power level from 0 (highest power) to 4 (lowest power).	R+B
`wlan radio <1:B Only|2:G Only|3:B+G|4:A Only>`	Sets the wireless radio mode. 1: 802.11b mode only 2: 802.11g mode only 3: 802.11b + 802.11g modes 4: 802.11a mode only.	R+B
`wlan rtsThreshold <256~2346>`	Sets the RTS/CTS threshold value.	R+B
`wlan removeSTA <mac-address>`	Disconnects a connected wireless station with the specified MAC address.	R+B
`wlan reset`	Resets the ZyWALL's wireless module.	R+B
`wlan scan`	Scans the environment and displays a recommended RF channel which is not used by other wireless APs in that area. This command works only when your wireless card is activated.	R+B
`wlan ssidprofile set <profile-name>`	Sets the wireless card to use the specified SSID profile.	R+B
`wlan ssidprofile show`	Displays the currently active SSID profile.	R+B

Table 81 General Wireless Commands (continued)

COMMAND	DESCRIPTION	M
`wlan version`	Displays the driver version number of the wireless card.	R+B
`wlan showBandInfo`	Displays the radio frequency band the wireless card is currently using.	R+B
`wlan counter`	Displays driver status.	R+B

The following section lists the commands deal with SSID profiles. ZyWALL supports 8 SSID profiles. Only one SSID profile is active at the same time.

Table 82 Wireless SSID Profile Commands

COMMAND	DESCRIPTION	M
`wcfg ssid <1~8> name <`*`name`*`>`	Sets the name for the specified SSID profile.	R+B
`wcfg ssid <1~8> ssid <`*`ssid`*`>`	Sets the SSID for the specified SSID profile.	R+B
`wcfg ssid <1~8> hidenssid <enable|disable>`	Sets whether the specified SSID profile's SSID is hidden (not broadcasted).	R+B
`wcfg ssid <1~8> security <`*`security-profile-name`*`>`	Binds the security profile with the specified SSID profile.	R+B
`wcfg ssid <1~8> macfilter <enable|disable>`	Enable or disable the MAC filter for the specified SSID profile.	R+B
`wcfg ssid <1~8> clear`	Resets the specified SSID profile to its default settings.	R+B
`wcfg ssid <1~8> save`	Saves the specified SSID profile configuration to the non-volatile memory.	R+B
`wcfg ssid <1~8> show`	Displays the configuration for the specified SSID profile.	R+B
`wcfg ssid display`	Displays all runtime SSID profile configuration.	R+B
`wcfg ssid spdisplay`	Displays all SSID profile configuration in the non-volatile memory.	R+B
`wcfg ssid saveall`	Saves all runtime SSID profile configuration to the non-volatile memory.	R+B

The following table describes the values required for many wireless WEP key setting commands. Other values are discussed with the relevant commands.

Table 83 Wireless WEP Key Command Input Values

LABEL	DESCRIPTION
`<key>`	This is a WEP key. You would have a different key length depending on the type of WEP key size you selected. If you use a 64-bit WEP key, enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you use a 128-bit WEP key, enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). If you use a 152-bit WEP key, enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F").

The following section lists the commands dealing with security profiles. The ZyWALL supports multiple security profiles. Only one security profile is active at one time.

Table 84 Wireless Security Profile Commands

COMMAND	DESCRIPTION	M
`wcfg security <1-8> name <name>`	Sets the security profile name.	R+B
`wcfg security <1-8> mode <none|wep|8021x-only|8021x-static64|8021x-static128|wpa|wpapsk|wpa2|wpa2mix|wpa2psk|wpa2pskmix>`	Sets the security mode for the specified security profile.	R+B
`wcfg security <1-8> wep keysize [64|128|152] [ascii|hex]`	Sets the WEP key length (in bits) and encoding method of WEP encryption for the specified security profile. `ascii|hex`: ASCII mode or Hex mode.	R+B
`wcfg security <1-8> wep auth [shared|auto]`	Sets the WEP authentication method for the specified security profile.	R+B
`wcfg security <1-8> wep key1 <key>`	Sets the WEP key1 for the specified security profile. Each security profile can use up to four keys. *key*: Refer to Table 83 on page 166.	R+B
`wcfg security <1-8> wep key2 <key>`	Sets the WEP key2 for the specified security profile. *key*: Refer to Table 83 on page 166.	R+B
`wcfg security <1-8> wep key3 <key>`	Sets the WEP key3 for the specified security profile. *key*: Refer to Table 83 on page 166.	R+B
`wcfg security <1-8> wep key4 <key>`	Sets the WEP key4 for the specified security profile. *key*: Refer to Table 83 on page 166.	R+B
`wcfg security <1-8> wep keyindex <1-4>`	Activates one of the four WEP keys to encrypt wireless data transmission.	R+B
`wcfg security <1-8> reauthtime <value>`	Sets the time interval for wireless re-authentication for the specified security profile.	R+B
`wcfg security <1-8> idletime <value>`	Sets the idle time before a forced de-association.	R+B
`wcfg security <1-8> groupkeytime <value>`	Sets the time interval for the WPA or WPA2 group key update. *value*: 600~65535 seconds.	R+B
`wcfg security <1-8> passphrase <value>`	Sets the passphrase when you selected security mode using `wpapsk`, `wpa2psk`, or `wpa2pskmix`. *value*: 8~63 alphanumeric characters.	R+B
`wcfg security <1-8> clear`	Sets the specified profile to its default value.	R+B
`wcfg security <1-8> save`	Saves the specified profile's configuration.	R+B
`wcfg security <1-8> show`	Displays the specified profile's configuration.	R+B
`wcfg security display`	Displays all runtime security profile settings.	R+B
`wcfg security saveall`	Saves all runtime wireless security settings to the non-volatile memory.	R+B

22.2 Command Examples

This example shows how to configure, save and display the settings of a wireless security profile. This example uses the following settings.

- Security profile name: Sec-01
- Security mode: WPA2 with Pre-Shared Key
- Group key update time interval: every 600 seconds
- Passphrase: aaaaaaaa

```
ras> wcfg security 1 name Sec-01
ras> wcfg security 1 mode wpa2psk
ras> wcfg security 1 groupkeytime 600
ras> wcfg security 1 passphrase aaaaaaaa
ras> wcfg security 1 save
Security policy 1 saved.
ras> wcfg security 1 show
---------------------------------------------------------------------------
  Index 1
  Name                        = Sec-01
  Security Mode               = wpa2psk
  [8021x/WPA/WPA2 setting]
  ReAuthentication timer      = 1800
  Idle timeout                = 3600
  WPA groupkey update timer = 600
  Pre-shared key              = aaaaaaaa
---------------------------------------------------------------------------
ras>
```

This example shows how to configure, save and display the settings of a wireless SSID profile. This example uses the following settings.

- SSID profile name: SSID-01
- SSID name: ZyWALL
- Security profile name: Sec-01
- Mac filter: disable

```
ras> wcfg ssid 1 name SSID-01
ras> wcfg ssid 1 ssid ZyWALL
ras> wcfg ssid 1 security Sec-01
ras> wcfg ssid 1 macfilter disable
ras> wcfg ssid 1 save
SSID policy 1 saved.
ras> wcfg ssid 1 show
---------------------------------------------------------------------------
  Index 1
  Name                           = SSID-01
  SSID                           = ZyWALL
  Ext. Security                  =
  QoS Mode                       = 0
  Security policy index(name)  = 1 (Sec-01)
---------------------------------------------------------------------------
ras>
```

23

WWAN Commands

Use these commands to configure wireless WAN settings on the ZyWALL.

23.1 Command Summary

The following table describes the values required for many `wwan` commands. Other values are discussed with the relevant commands.

Table 85 wwan Command Input Values

LABEL	DESCRIPTION
networkmodeindex	Specifies the index number of a listed network mode. You can find a list of network types by entering the command "`wwan card networkMode show`".
string	Enter a name with <31 ASCII characters unless otherwise specified.

The following section lists the commands for this feature.

Table 86 wwan Command Summary

COMMAND	DESCRIPTION	M
`wwan card networkMode change [`*networkmodeindex*`]`	Changes the network type.	R
`wwan card networkMode show`	Shows a numbered list of available network types. The network type available depends on the type of 3G card installed, for example, UMTS, HSDPA, GPRS, EDGE, GSM.	R
`wwan card serviceProv change [`*networkmodeindex*`]`	Changes the service provider.	R
`wwan card serviceProv show`	Scans for and shows a numbered list of the available cellular service providers.	R
`wwan card slot`	Shows information on the slot interface, for example, PCMCIA.	R
`wwan config apn <`*string*`>`	Sets the Access Point Name (APN) for an access point on a GSM network.	R
`wwan config authType [1|2|3|4]`	Sets the PPP authentication type. 1. None 2. CHAP only 3. PAP only 4. CHAP or PAP If 1.None is selected, no password or user name is required.	R

Table 86 wwan Command Summary (continued)

COMMAND	DESCRIPTION	M
`wwan config budgetCtrl data dir [1|2|3]`	Sets whether either transmitted (Tx) or received (Rx), or both Tx/Rx data should be counted for budget purposes. 1:Tx 2:Rx 3:Tx and Rx	R
`wwan config budgetCtrl data enable [on|off]`	Enables the recording of the amount of Tx/Rx data. This information is used for budget management.	R
`wwan config budgetCtrl data quota [`*`data_quota`*`]`	Sets the data limit measured in megabytes. *`data_quota`* may be between 1 Mb to 100 Gb.	R
`wwan config budgetCtrl enable [on|off]`	Enables budget control.	R
`wwan config budgetCtrl highLimit`	Sets the upper limit for the data budget.	R
`wwan config budgetCtrl highLimit alert [on|off]`	Sends an alert if the data limit is exceeded.	R
`wwan config budgetCtrl highLimit AllowNewConn [on|off]`	Allows new 3G connections to be established when the data limit is exceeded.	R
`wwan config budgetCtrl highLimit KeepCurrConn [on|off]`	Keeps the current 3G connection (ON) or drops it (OFF) if the data limit is exceeded.	R
`wwan config budgetCtrl highLimit log [on|off]`	Sends a log if the data limit is exceeded.	R
`wwan config budgetCtrl lowLimit`	Sets a data level at which to send an alert or log before the maximum data limit is reached.	R
`wwan config budgetCtrl lowLimit alert [on|off]`	Sends an alert if the warning level is reached.	R
`wwan config budgetCtrl lowLimit data <%>`	Sets a warning level as a percentage of the data limit.	R
`wwan config budgetCtrl lowLimit log [on|off]`	Sends a log if the warning level is exceeded.	R
`wwan config budgetCtrl lowLimit time <%>`	Sets a time for a warning as a percentage of the Internet access time limit.	R
`wwan config budgetCtrl resetDay <`*`day`*`>`	Sets the day of each month to reset the budget counter.	R
`wwan config budgetCtrl time enable [on|off]`	Enables the recording of time spent accessing the Internet for budget control.	R
`wwan config budgetCtrl time quota [`*`time_in_hours`*`]`	Sets the time limit for Internet access in hours. Maximum is 672 hours.	R
`wwan config enable [on|off]`	Enables 3G Wireless WAN.	R
`wwan config idleTimeout <`*`time_in_seconds`*`>`	Sets the maximum period the connection may remain idle before disconnection. *`time_in_seconds`* may be 1-9999 seconds.	R
`wwan config multicast enable [on|off]`	Enables multicast for 3G wireless WAN.	R
`wwan config multicast version [1|2]`	Sets multicast to IGMP (Internet Group Management Protocol) version 1 or 2. 1:IGMPv1 2:IGMPv2	R

Table 86 wwan Command Summary (continued)

COMMAND	DESCRIPTION	M
`wwan config nailUp [on|off]`	Enables a nailed up (always on) connection.	R
`wwan config nat [on|off]`	Enables NAT (Network Address Translation).	R
`wwan config password <string>`	Sets the password for PPP authentication.	R
`wwan config phoneNumber <string>`	Sets the phone number for access to a cellular network.	R
`wwan config pin <string>`	Sets the PIN code (4~8 digits) for a GSM SIM card.	R
`wwan config username <string>`	Sets the user name for PPP authentication.	R
`wwan config wanIpAddr <ip>`	Sets the IP address of the WAN. The WAN IP address must first be set to fixed.	R
`wwan config wanIpAssign [1|2]`	Sets whether the WAN IP address is (1) automatically obtained, or (2) fixed.	R
`wwan load`	Loads the original configuration of the device from the ROM. This must be done before the device can be configured and/or saved.	R
`wwan profile select [index]`	A 3G card must be installed to use this command. Specifies the profile of settings in the installed 3G card to use for the 3G connection. 0 disables profile selection so the ZyWALL uses the APN, username, and password configured in the web configurator WAN2 screen.	R
`wwan profile show`	A 3G card must be installed to use this command. Displays the profile settings in the installed 3G card.	R
`wwan save`	Saves the configuration.	R

The following table shows a list of default values.

Table 87 wwan Default Values

VARIABLE	DEFAULT VALUE
`3G WWAN`	off
`Budget control enabled`	3: TxAndRx
`budgetCtrl data enable`	off
`budgetCtrl time enable`	off
`idle Timeout`	100 seconds
`nail Up`	off
`NAT`	on
`PPP authentication type`	None
`WAN IP address obtain`	1:Auto
`wanIPAddress`	0.0.0.0
`WWAN multicast enabled`	off

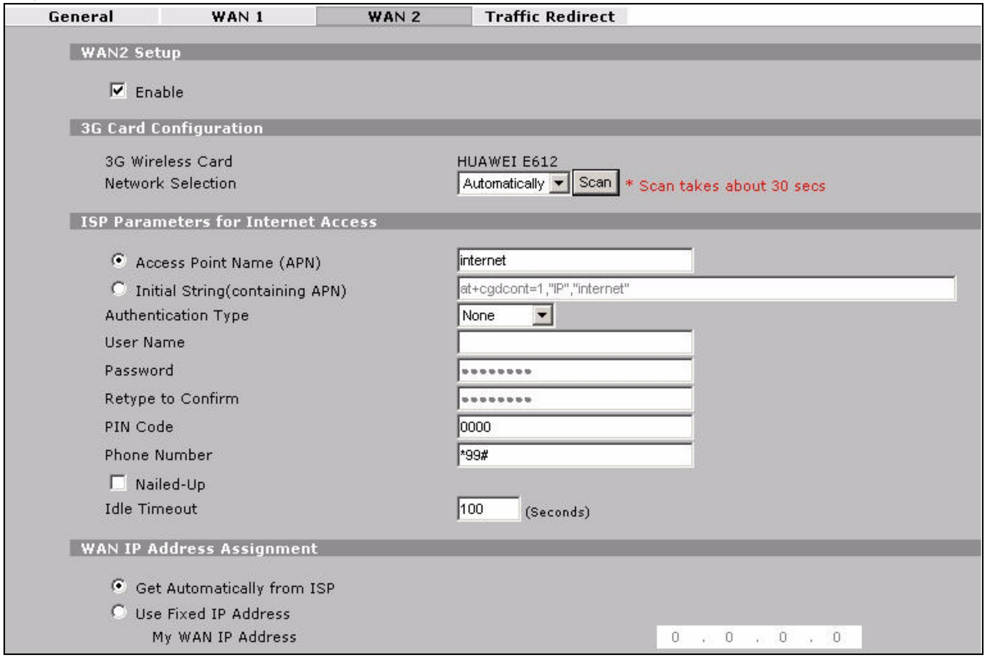
23.2 Command Examples

If using 3G cards such as the AC850, AC875, E612, E620, or OptionGT HSDPA 7.2, type the commands below to configure 3G WWAN.

```
ras> wwan load
ras> wwan config apn internet
ras> wwan config authType 3
ras> wwan config enable on
ras> wwan config nat on
ras> wwan config nailUp off
ras> wwan config phoneNumber *99#
ras> wwan config pin 0000
ras> wwan config wanIpAssign 1
ras> wwan config budget enable on
ras> wwan config budget time enable on
ras> wwan config budget time quota 10
ras> wwan config budget highLimit log on
ras> wwan config budget lowLimit timePercent
ras> wwan config budget lowLimit timePercent 60
ras> wwan config budget lowLimit log on
ras> wwan config budget resetDay 6
ras> wwan save
```

The following screens show the same configuration using the web configurator.

Figure 10 WWAN configuration example



WAN2 Setup

☑ Enable

3G Card Configuration

3G Wireless Card	HUAWEI E612
Network Selection	Automatically * Scan takes about 30 secs

ISP Parameters for Internet Access

● Access Point Name (APN)	internet
○ Initial String(containing APN)	at+cgdcont=1,"IP","internet"
Authentication Type	None
User Name	
Password	••••••••
Retype to Confirm	••••••••
PIN Code	0000
Phone Number	*99#
□ Nailed-Up	
Idle Timeout	100 (Seconds)

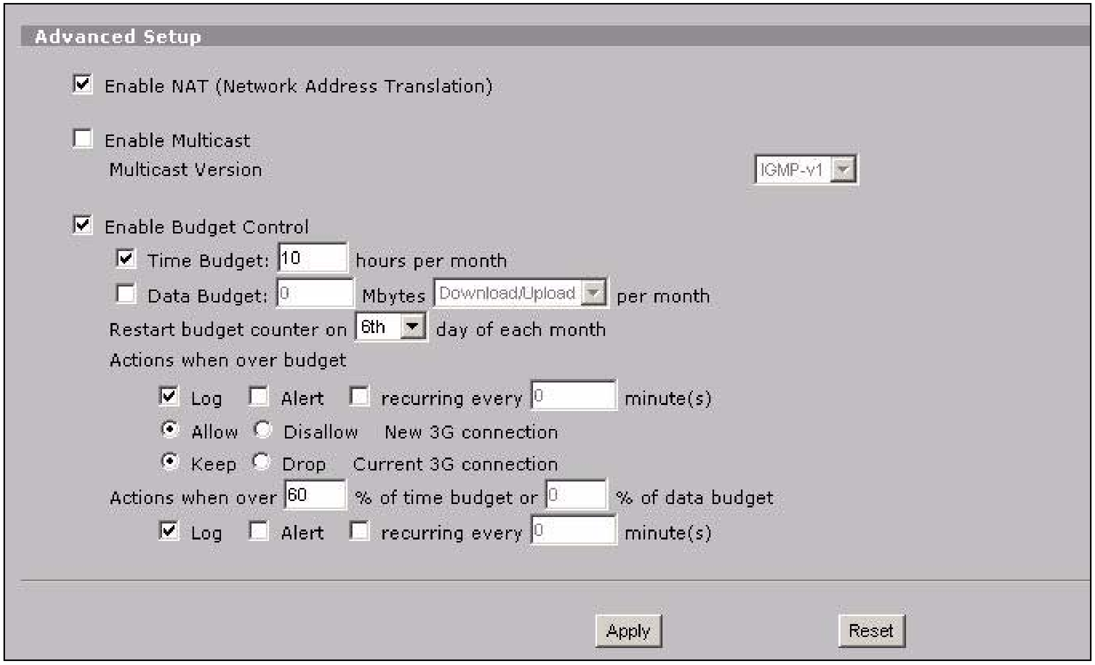
WAN IP Address Assignment

● Get Automatically from ISP

○ Use Fixed IP Address

My WAN IP Address 0 . 0 . 0 . 0

Figure 11 WWAN configuration example



Advanced Setup

☑ Enable NAT (Network Address Translation)

□ Enable Multicast

Multicast Version IGMP-v1

☑ Enable Budget Control

☑ Time Budget: 10 hours per month

□ Data Budget: 0 Mbytes Download/Upload per month

Restart budget counter on 6th day of each month

Actions when over budget

☑ Log □ Alert □ recurring every 0 minute(s)

● Allow ○ Disallow New 3G connection

● Keep ○ Drop Current 3G connection

Actions when over 60 % of time budget or 0 % of data budget

☑ Log □ Alert □ recurring every 0 minute(s)

PART III

Appendices and Index of Commands

A

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍
受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

在 5250MHz~5350MHz 頻帶內操作之無線資訊傳輸設備，限於室內使用。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz and 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This device has been designed for the WLAN 5 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

B

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: http://www.zyxel.cn

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Taiwan

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: http://www.zyxel.com.tw
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Turkey

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: http:www.zyxel.com.tr
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 0845 122 0301 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index of Commands

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.